CS4415 – FINAL PROJECT

By: Julia Walker, Amir David, Matthew Hunter

Overview

- Attack Description
- Initial Thoughts
- Project Description
- Analysis
- Features
  - *Number of active IP Connections*
  - *Segmented TCP Packets*

Attack Description

Denial of Service

- Denial of Service attacks attempt to disrupt or block the availability of a network service by exhausting the service’s resources

- The attacker creates large amounts of traffic directed at the network until the network crashes

- Legitimate users are unable to access the network

Initial Thoughts

- Based on our initial thoughts and assumptions about DoS attacks we develop 3 possible features
  - *Number of connections per minute*
  - *Length of time the request is open*
  - *Amount of requests per IP connection*

- Through traffic analysis of simulated attacks, and research about slowloris we developed new features that are more specific to a Slowloris attack.

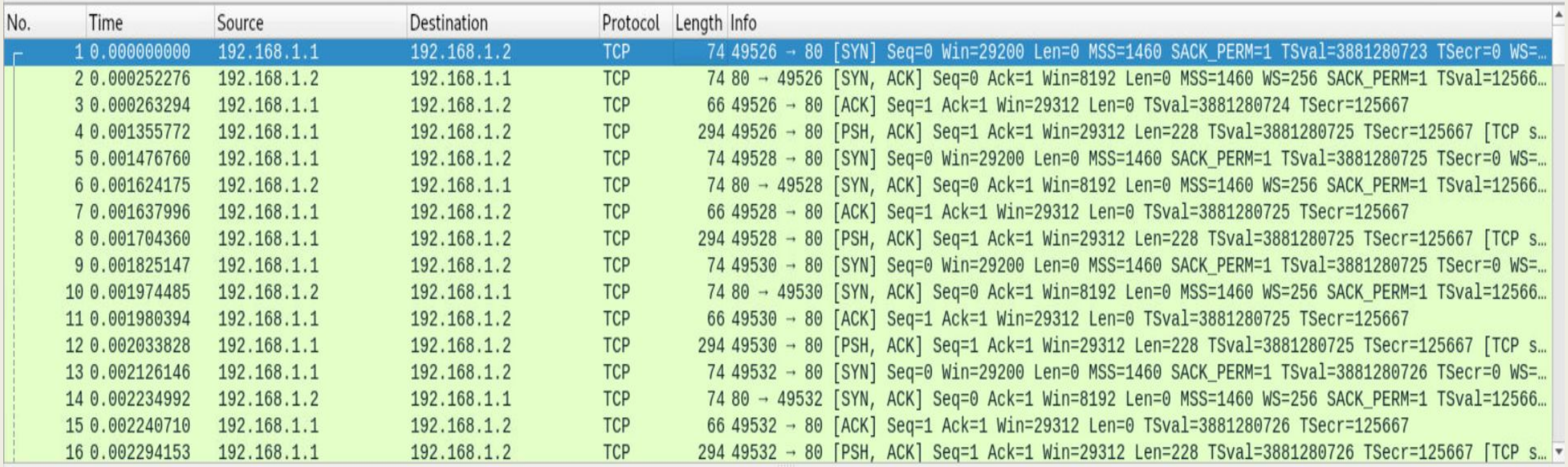
Project Description

- Our project utilized Slowloris to simulate the attacks

- Analysis was done in Wireshark

- The program is written in Python and uses netstat and tshark for the feature detection and traffic flows

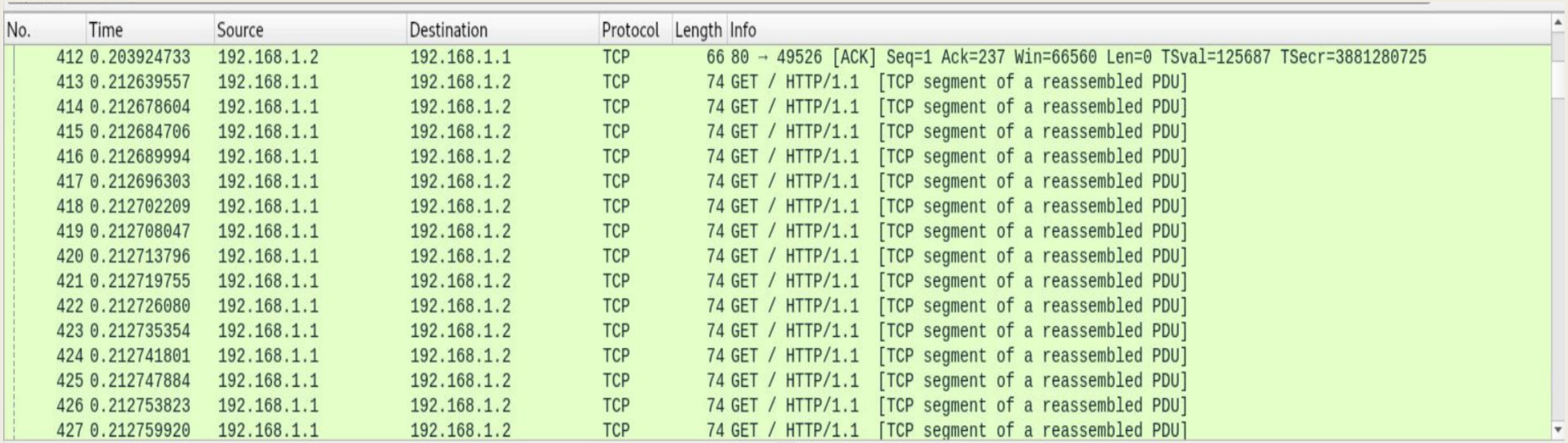
Analysis of a Slowloris Attack



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.1	192.168.1.2	TCP	74	49526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3881280723 TSecr=0 WS=…
2	0.000252276	192.168.1.2	192.168.1.1	TCP	74	80 → 49526 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=12566…
3	0.000263294	192.168.1.1	192.168.1.2	TCP	66	49526 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3881280724 TSecr=125667
4	0.001355772	192.168.1.1	192.168.1.2	TCP	294	49526 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=228 TSval=3881280725 TSecr=125667 [TCP s…
5	0.001476760	192.168.1.1	192.168.1.2	TCP	74	49528 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3881280725 TSecr=0 WS=…
6	0.001624175	192.168.1.2	192.168.1.1	TCP	74	80 → 49528 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=12566…
7	0.001637996	192.168.1.1	192.168.1.2	TCP	66	49528 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3881280725 TSecr=125667
8	0.001704360	192.168.1.1	192.168.1.2	TCP	294	49528 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=228 TSval=3881280725 TSecr=125667 [TCP s…
9	0.001825147	192.168.1.1	192.168.1.2	TCP	74	49530 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3881280725 TSecr=0 WS=…
10	0.001974485	192.168.1.2	192.168.1.1	TCP	74	80 → 49530 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=12566…
11	0.001980394	192.168.1.1	192.168.1.2	TCP	66	49530 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3881280725 TSecr=125667
12	0.002033828	192.168.1.1	192.168.1.2	TCP	294	49530 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=228 TSval=3881280725 TSecr=125667 [TCP s…
13	0.002126146	192.168.1.1	192.168.1.2	TCP	74	49532 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3881280726 TSecr=0 WS=…
14	0.002234992	192.168.1.2	192.168.1.1	TCP	74	80 → 49532 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=12566…
15	0.002240710	192.168.1.1	192.168.1.2	TCP	66	49532 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3881280726 TSecr=125667
16	0.002294153	192.168.1.1	192.168.1.2	TCP	294	49532 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=228 TSval=3881280726 TSecr=125667 [TCP s…

Slowloris utilizing a series of TCP handshakes to maintain an open connection using the [PSH, ACK] flag. This exhausts the resources of the server

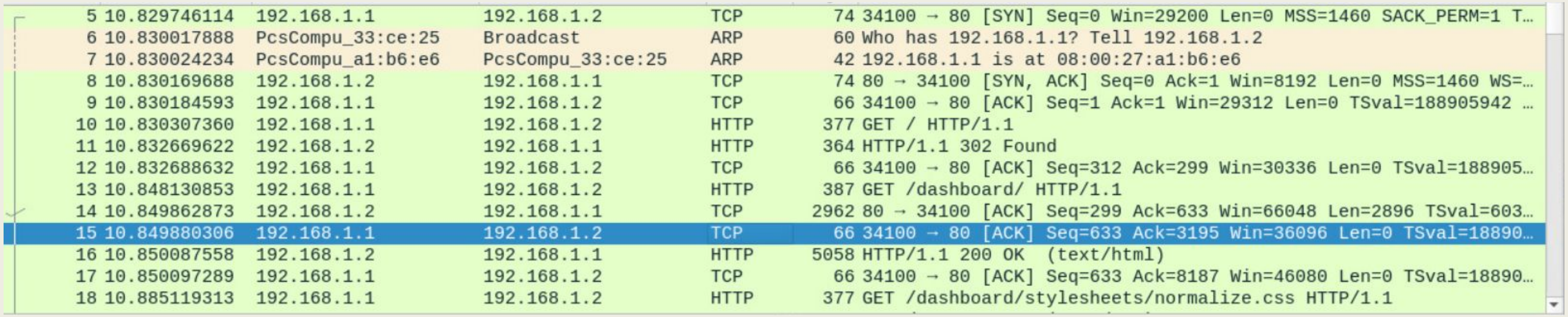
Analysis of a Slowloris Attack



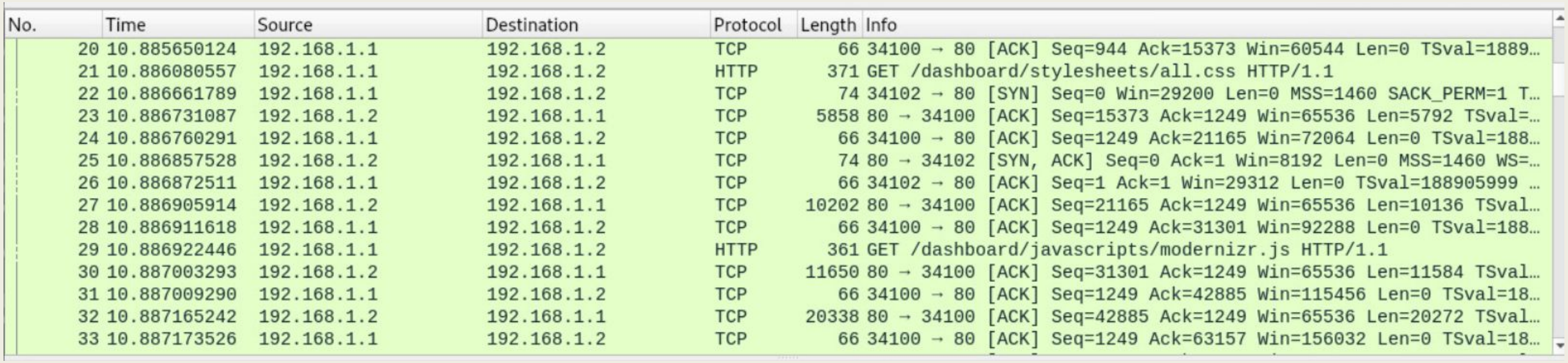
No.	Time	Source	Destination	Protocol	Length	Info
412	0.203924733	192.168.1.2	192.168.1.1	TCP	66	80 → 49526 [ACK] Seq=1 Ack=237 Win=66560 Len=0 TSval=125687 TSecr=3881280725
413	0.212639557	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
414	0.212678604	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
415	0.212684706	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
416	0.212689994	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
417	0.212696303	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
418	0.212702209	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
419	0.212708047	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
420	0.212713796	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
421	0.212719755	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
422	0.212726080	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
423	0.212735354	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
424	0.212741801	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
425	0.212747884	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
426	0.212753823	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]
427	0.212759920	192.168.1.1	192.168.1.2	TCP	74	GET / HTTP/1.1 [TCP segment of a reassembled PDU]

Slowloris sends multiple segmented TCP packets

Analysis of normal network traffic



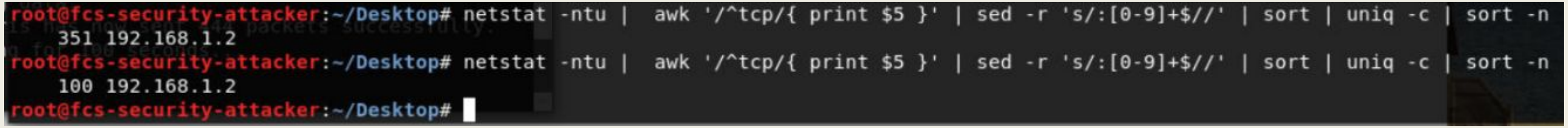
```
 5 10.829746114  192.168.1.1          192.168.1.2          TCP        74 34100 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 T…
 6 10.830017888  PcsCompu_33:ce:25    Broadcast            ARP        60 Who has 192.168.1.1? Tell 192.168.1.2
 7 10.830024234  PcsCompu_a1:b6:e6    PcsCompu_33:ce:25    ARP        42 192.168.1.1 is at 08:00:27:a1:b6:e6
 8 10.830169688  192.168.1.2          192.168.1.1          TCP        74 80 → 34100 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=…
 9 10.830184593  192.168.1.1          192.168.1.2          TCP        66 34100 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=188905942 …
10 10.830307360  192.168.1.1          192.168.1.2          HTTP      377 GET / HTTP/1.1
11 10.832669622  192.168.1.2          192.168.1.1          HTTP      364 HTTP/1.1 302 Found
12 10.832688632  192.168.1.1          192.168.1.2          TCP        66 34100 → 80 [ACK] Seq=312 Ack=299 Win=30336 Len=0 TSval=188905…
13 10.848130853  192.168.1.1          192.168.1.2          HTTP      387 GET /dashboard/ HTTP/1.1
14 10.849862873  192.168.1.2          192.168.1.1          TCP      2962 80 → 34100 [ACK] Seq=299 Ack=633 Win=66048 Len=2896 TSval=603…
15 10.849880306  192.168.1.1          192.168.1.2          TCP        66 34100 → 80 [ACK] Seq=633 Ack=3195 Win=36096 Len=0 TSval=18890…
16 10.850087558  192.168.1.2          192.168.1.1          HTTP     5058 HTTP/1.1 200 OK  (text/html)
17 10.850097289  192.168.1.1          192.168.1.2          TCP        66 34100 → 80 [ACK] Seq=633 Ack=8187 Win=46080 Len=0 TSval=18890…
18 10.885119313  192.168.1.1          192.168.1.2          HTTP      377 GET /dashboard/stylesheets/normalize.css HTTP/1.1
```



```
No.  Time          Source               Destination          Protocol Length Info
 20 10.885650124  192.168.1.1          192.168.1.2          TCP         66 34100 → 80 [ACK] Seq=944 Ack=15373 Win=60544 Len=0 TSval=1889…
 21 10.886080557  192.168.1.1          192.168.1.2          HTTP       371 GET /dashboard/stylesheets/all.css HTTP/1.1
 22 10.886661789  192.168.1.1          192.168.1.2          TCP         74 34102 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 T…
 23 10.886731087  192.168.1.2          192.168.1.1          TCP       5858 80 → 34100 [ACK] Seq=15373 Ack=1249 Win=65536 Len=5792 TSval=…
 24 10.886760291  192.168.1.1          192.168.1.2          TCP         66 34100 → 80 [ACK] Seq=1249 Ack=21165 Win=72064 Len=0 TSval=188…
 25 10.886857528  192.168.1.2          192.168.1.1          TCP         74 80 → 34102 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=…
 26 10.886872511  192.168.1.1          192.168.1.2          TCP         66 34102 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=188905999 …
 27 10.886905914  192.168.1.2          192.168.1.1          TCP      10202 80 → 34100 [ACK] Seq=21165 Ack=1249 Win=65536 Len=10136 TSval…
 28 10.886911618  192.168.1.1          192.168.1.2          TCP         66 34100 → 80 [ACK] Seq=1249 Ack=31301 Win=92288 Len=0 TSval=188…
 29 10.886922446  192.168.1.1          192.168.1.2          HTTP       361 GET /dashboard/javascripts/modernizr.js HTTP/1.1
 30 10.887003293  192.168.1.2          192.168.1.1          TCP      11650 80 → 34100 [ACK] Seq=31301 Ack=1249 Win=65536 Len=11584 TSval…
 31 10.887009290  192.168.1.1          192.168.1.2          TCP         66 34100 → 80 [ACK] Seq=1249 Ack=42885 Win=115456 Len=0 TSval=18…
 32 10.887165242  192.168.1.2          192.168.1.1          TCP      20338 80 → 34100 [ACK] Seq=42885 Ack=1249 Win=65536 Len=20272 TSval…
 33 10.887173526  192.168.1.1          192.168.1.2          TCP         66 34100 → 80 [ACK] Seq=1249 Ack=63157 Win=156032 Len=0 TSval=18…
```

Feature One: Number of Connections

- During an attack, the attacker opens a large number of IP connections with the server
- Our solution detects the number of open IP connections
- If the number of connections exceeds a certain threshold, a warning message is displayed indicating the number of connections.
- The threshold was calculated based on the number of connections above which the operation of the server is disrupted.

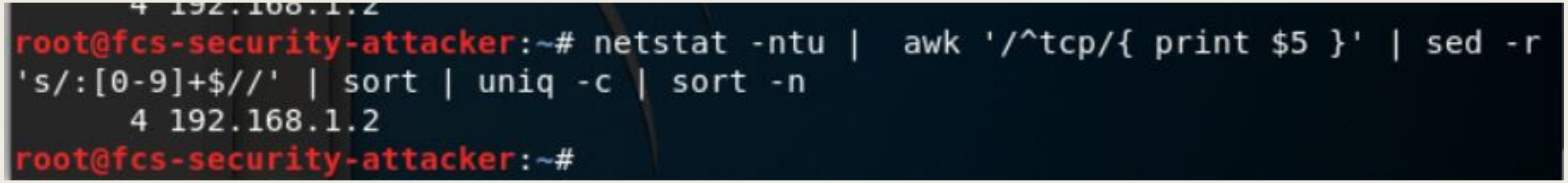


```
root@fcs-security-attacker:~/Desktop# netstat -ntu |  awk '/^tcp/{ print $5 }' | sed -r 's/:[0-9]+$//' | sort | uniq -c | sort -n
    351 192.168.1.2
root@fcs-security-attacker:~/Desktop# netstat -ntu |  awk '/^tcp/{ print $5 }' | sed -r 's/:[0-9]+$//' | sort | uniq -c | sort -n
    100 192.168.1.2
root@fcs-security-attacker:~/Desktop# 
```

An example of the number of IP connection opened by Slowloris during an attack

Number of Connections

Normal Traffic

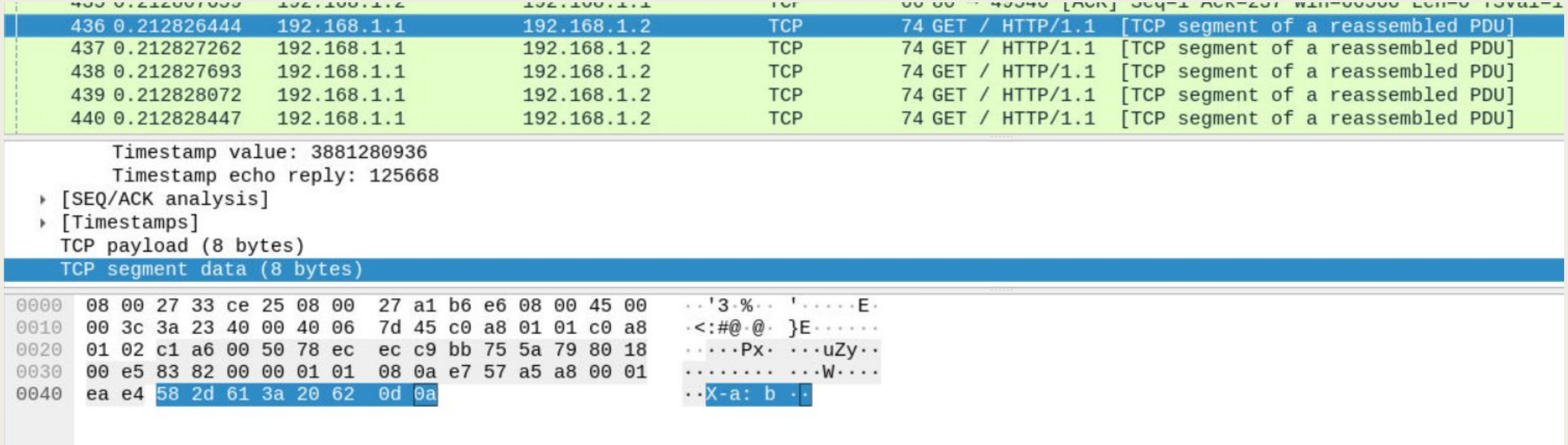


```
     4 192.168.1.2
root@fcs-security-attacker:~# netstat -ntu |  awk '/^tcp/{ print $5 }' | sed -r
's/:[0-9]+$//' | sort | uniq -c | sort -n
     4 192.168.1.2
root@fcs-security-attacker:~#
```

An example of the number of connections to the server during normal traffic

Feature Two: Segmented TCP Packets

- During the attack, Slowloris sends many segmented TCP packets.
- The segmented packets’ headers are incomplete because they end with the sequence 0d0a (“CRLF”) instead of 0d0a0d0a (“CRLF CRLF”).
- This exhausts the server resources.



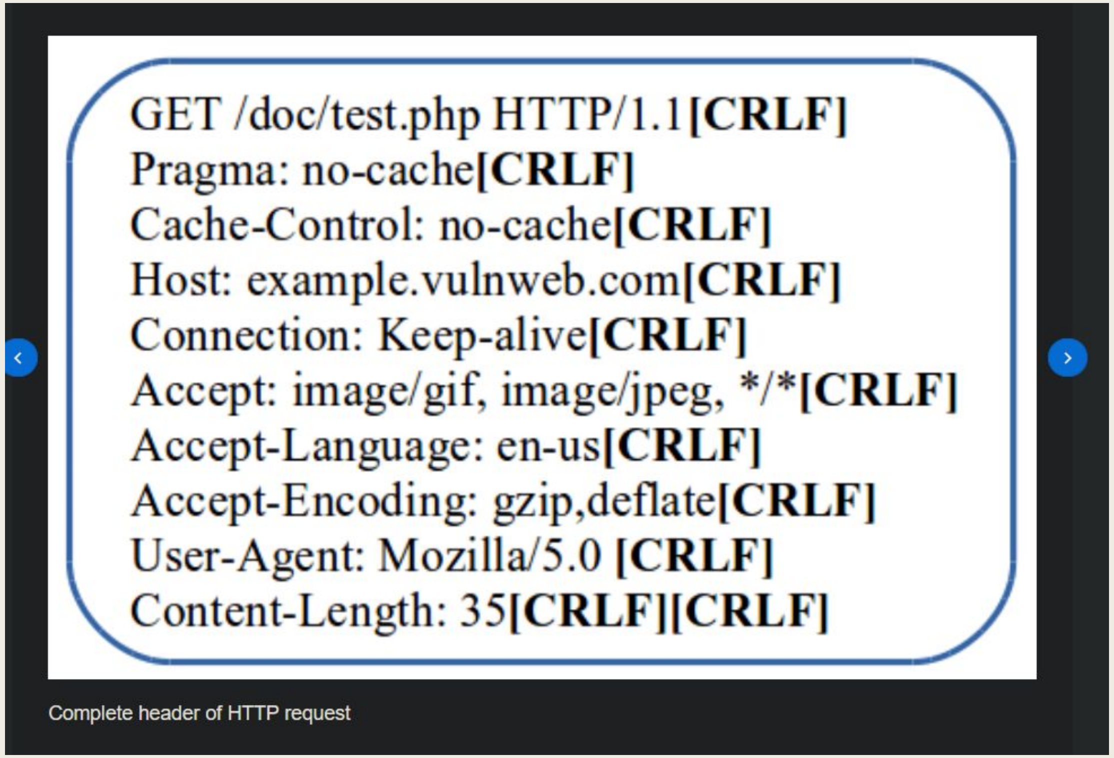
```
436 0.212826444   192.168.1.1        192.168.1.2        TCP       74 GET / HTTP/1.1  [TCP segment of a reassembled PDU]
437 0.212827262   192.168.1.1        192.168.1.2        TCP       74 GET / HTTP/1.1  [TCP segment of a reassembled PDU]
438 0.212827693   192.168.1.1        192.168.1.2        TCP       74 GET / HTTP/1.1  [TCP segment of a reassembled PDU]
439 0.212828072   192.168.1.1        192.168.1.2        TCP       74 GET / HTTP/1.1  [TCP segment of a reassembled PDU]
440 0.212828447   192.168.1.1        192.168.1.2        TCP       74 GET / HTTP/1.1  [TCP segment of a reassembled PDU]

        Timestamp value: 3881280936
        Timestamp echo reply: 125668
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (8 bytes)
    TCP segment data (8 bytes)

0000  08 00 27 33 ce 25 08 00  27 a1 b6 e6 08 00 45 00   ··'3·%·· '·····E·
0010  00 3c 3a 23 40 00 40 06  7d 45 c0 a8 01 01 c0 a8   ·<:#@·@· }E······
0020  01 02 c1 a6 00 50 78 ec  ec c9 bb 75 5a 79 80 18   ·····Px· ···uZy··
0030  00 e5 83 82 00 00 01 01  08 0a e7 57 a5 a8 00 01   ········ ···W····
0040  ea e4 58 2d 61 3a 20 62  0d 0a                     ··X-a: b ··
```

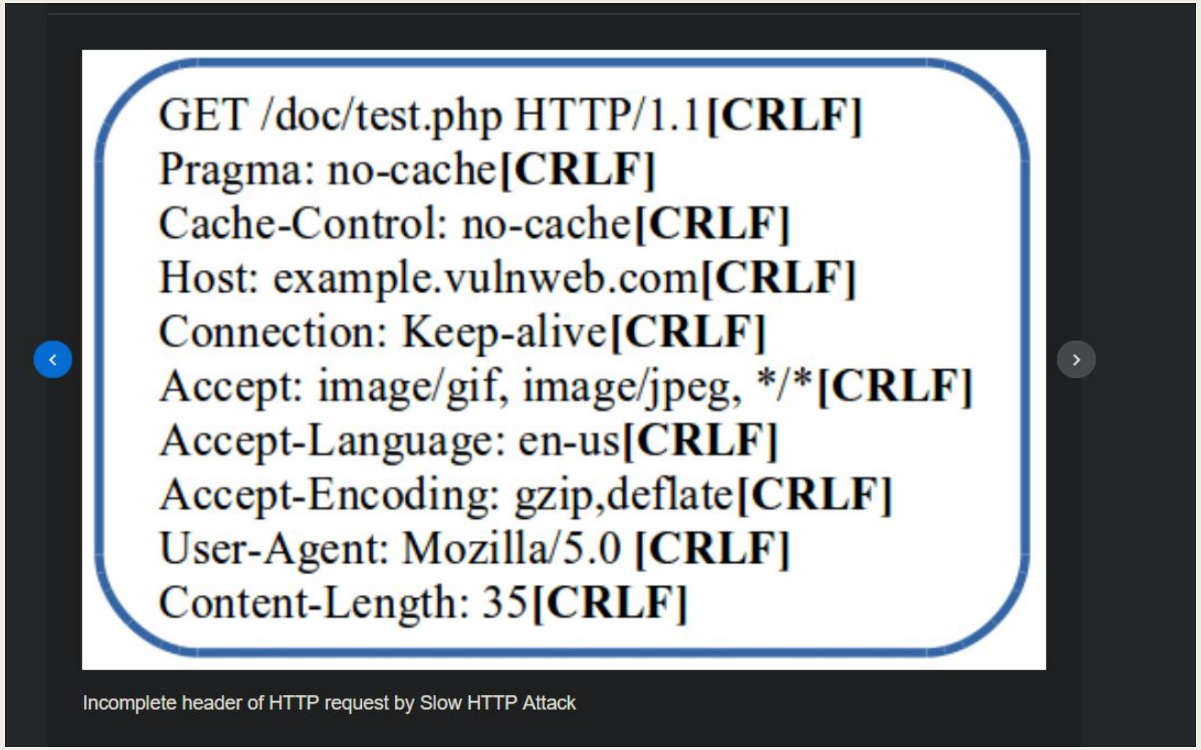
Segmented TCP packets

Complete vs. Incomplete Headers



```
GET /doc/test.php HTTP/1.1[CRLF]
Pragma: no-cache[CRLF]
Cache-Control: no-cache[CRLF]
Host: example.vulnweb.com[CRLF]
Connection: Keep-alive[CRLF]
Accept: image/gif, image/jpeg, */*[CRLF]
Accept-Language: en-us[CRLF]
Accept-Encoding: gzip,deflate[CRLF]
User-Agent: Mozilla/5.0 [CRLF]
Content-Length: 35[CRLF][CRLF]
```

Complete header of HTTP request



```
GET /doc/test.php HTTP/1.1[CRLF]
Pragma: no-cache[CRLF]
Cache-Control: no-cache[CRLF]
Host: example.vulnweb.com[CRLF]
Connection: Keep-alive[CRLF]
Accept: image/gif, image/jpeg, */*[CRLF]
Accept-Language: en-us[CRLF]
Accept-Encoding: gzip,deflate[CRLF]
User-Agent: Mozilla/5.0 [CRLF]
Content-Length: 35[CRLF]
```

Incomplete header of HTTP request by Slow HTTP Attack