The project discription :  
  
The goal : protect http server from Dos, using hadoop and snort  
  
1- Fist we  simulate the Dos attack by using hping3  
  
2- Then we log the packets by snort , and send the log file to hadoop  
  
3- In hadoop we write a mapreduce code to detect the Dos attack by count the number of http per second, and if it was greater than specific number, we consider it  DOS attack , and  generate an alert contain the number of http per second, the source and destination adress,ports, the time and date of the attack

I want to add this:

1- total date and time(time from begin the attack to  time when the attak last)  
2- we defined DOS attack more than 100 instead of 5000  
3- The total number of attack packets   
  
\*- the output file as bellow:  
  
  
  
An attempt to HTTP Dos attack discoverd in date/time //((time from begin the attack - time when the attack finsh)  
  
Type of attack : web server denial of service attack buffer over flow - number of packet in each second exceed 100 http  
  
The total number of attack packets is :   // total from the start to the end  
  
The attacker source address is:  
  
Destination adrress:  
  
  
  
Attack details per seconds:  
  
2017-06-13 05:12:28 192.168.5.104    5100  
2017-06-13 05:12:29 192.168.5.104    1777  
2017-06-13 05:12:30 192.168.5.104    8940  
2017-06-13 05:12:31 192.168.5.104    10438  
2017-06-13 05:12:32 192.168.5.104    9615  
2017-06-13 05:12:33 192.168.5.104    9924  
2017-06-13 05:12:34 192.168.5.104    10345  
2017-06-13 05:12:35 192.168.5.104    6274  
2017-06-13 05:12:36 192.168.5.104    4128  
2017-06-13 05:12:37 192.168.5.104    10340  
2017-06-13 05:12:38 192.168.5.104    9975  
2017-06-13 05:12:39 192.168.5.104    9887  
2017-06-13 05:12:40 192.168.5.104    9863  
2017-06-13 05:12:41 192.168.5.104    7153

Hi Guo, no im not busy now  
  
I mean this:  
if the numer of packer per second greater than 100 we consider it Dos attack and print this information in the output file like this :  
  
  
  
print this message :  
  
An attempt to HTTP Dos attack discoverd   
Type of attack : web server denial of service attack buffer over flow  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
add this information :  
  
1- i want the time when the attack start until the time of end , in all file not per second  
  
example:  
  
Attack start at : 2017-06-13 05:12:28.449650   
And End at : 2017-06-13 05:12:41.713131

There need three mapreduce:

1 count the time in the files

2 count the counts in the time

3 details   
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
2- the totalcount of all packets in the file (not total in each second, total packet in total time)  
  
for example:  
  
total packet count: 133843 http reqest in 13 mintues  
  
from 05:12:28.449650 - 05:12:41.713131  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
The attacker source address is: "the ip of source"   
  
Destination adrress:   "the ip of Destination"  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
  
in addition to the pervious code that count the packet per second:  
  
  
Attack details per seconds:  
  
2017-06-13 05:12:28 192.168.5.104    5100  
2017-06-13 05:12:29 192.168.5.104    1777  
2017-06-13 05:12:30 192.168.5.104    8940  
2017-06-13 05:12:31 192.168.5.104    10438  
2017-06-13 05:12:32 192.168.5.104    9615  
2017-06-13 05:12:33 192.168.5.104    9924  
2017-06-13 05:12:34 192.168.5.104    10345  
2017-06-13 05:12:35 192.168.5.104    6274  
2017-06-13 05:12:36 192.168.5.104    4128  
2017-06-13 05:12:37 192.168.5.104    10340  
2017-06-13 05:12:38 192.168.5.104    9975  
2017-06-13 05:12:39 192.168.5.104    9887  
2017-06-13 05:12:40 192.168.5.104    9863  
2017-06-13 05:12:41 192.168.5.104    7153