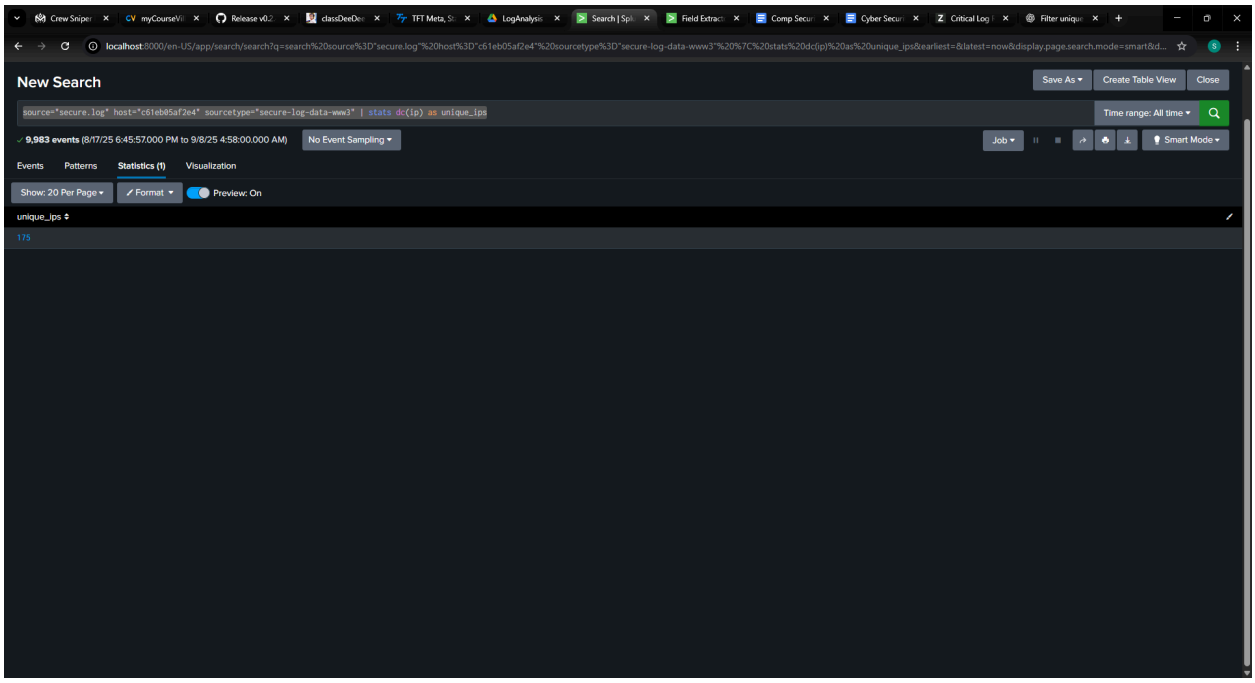
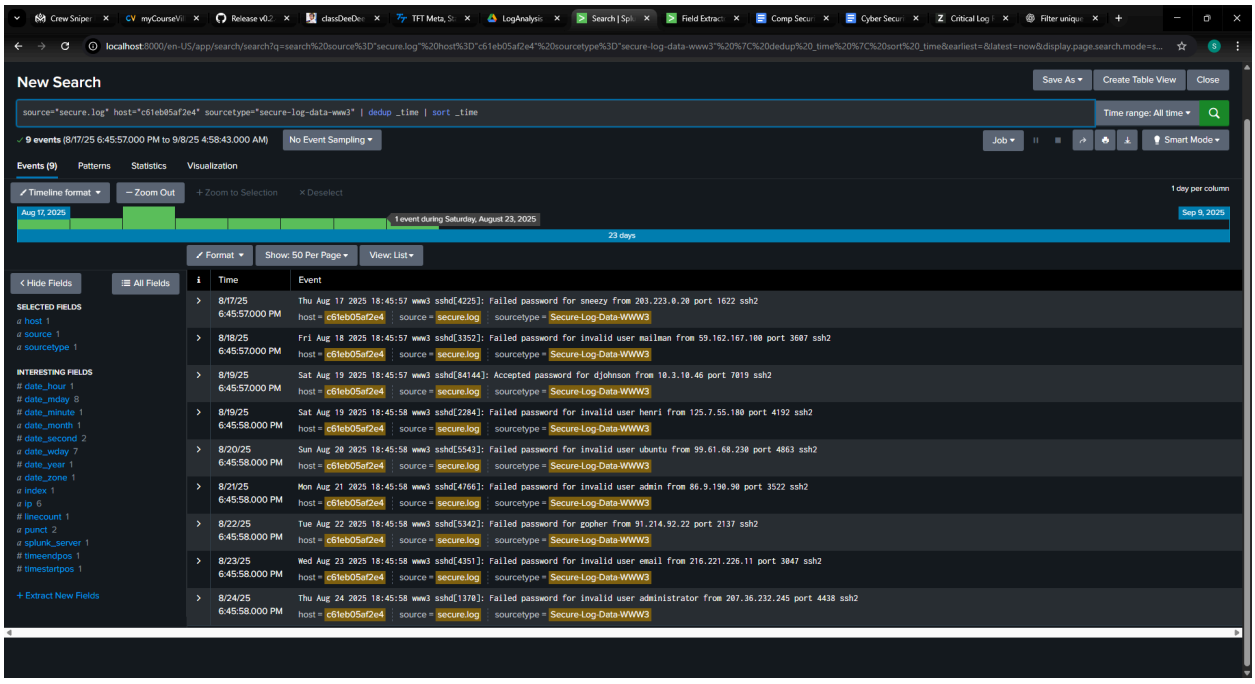
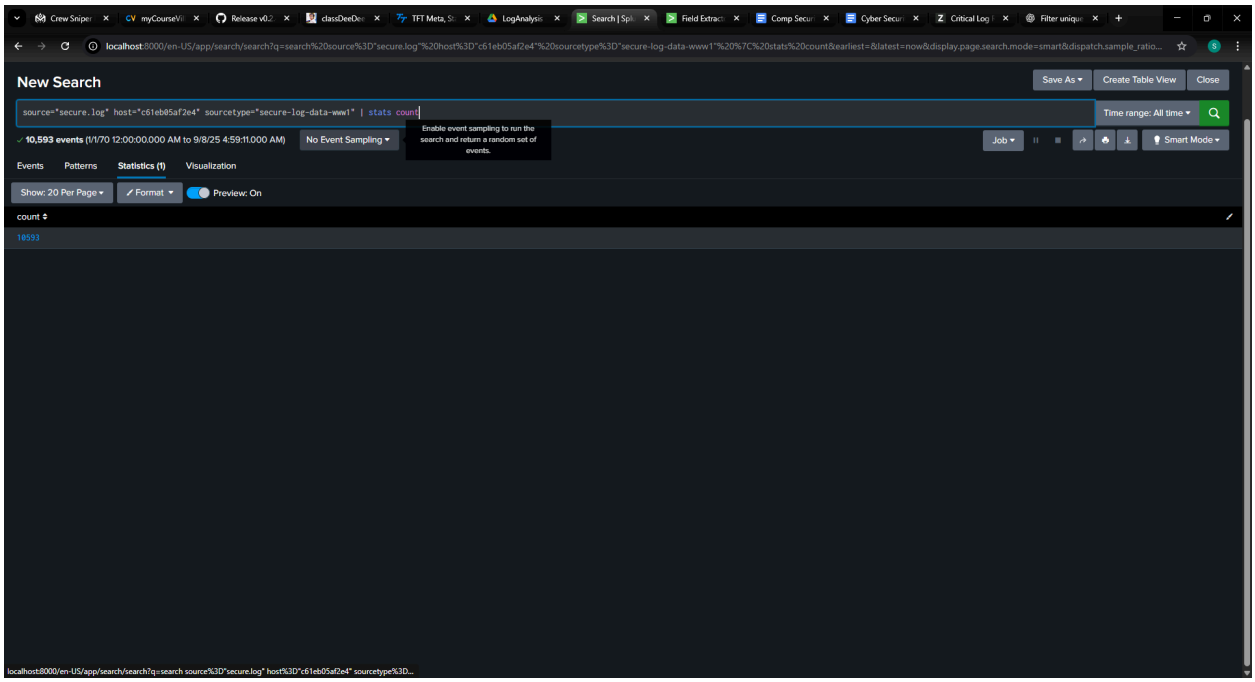
1) How many hackers are trying to get access to our servers? And how many attempts are there? Explain/define how you count distinct hackers.
Answer There is 182 different suspect (login failed) the filtered is source="secure.log" host="c61eb05af2e4" sourcetype="Secure-Log-Data-WWW2"| dedup ip (extract field is required failed password / field ip)



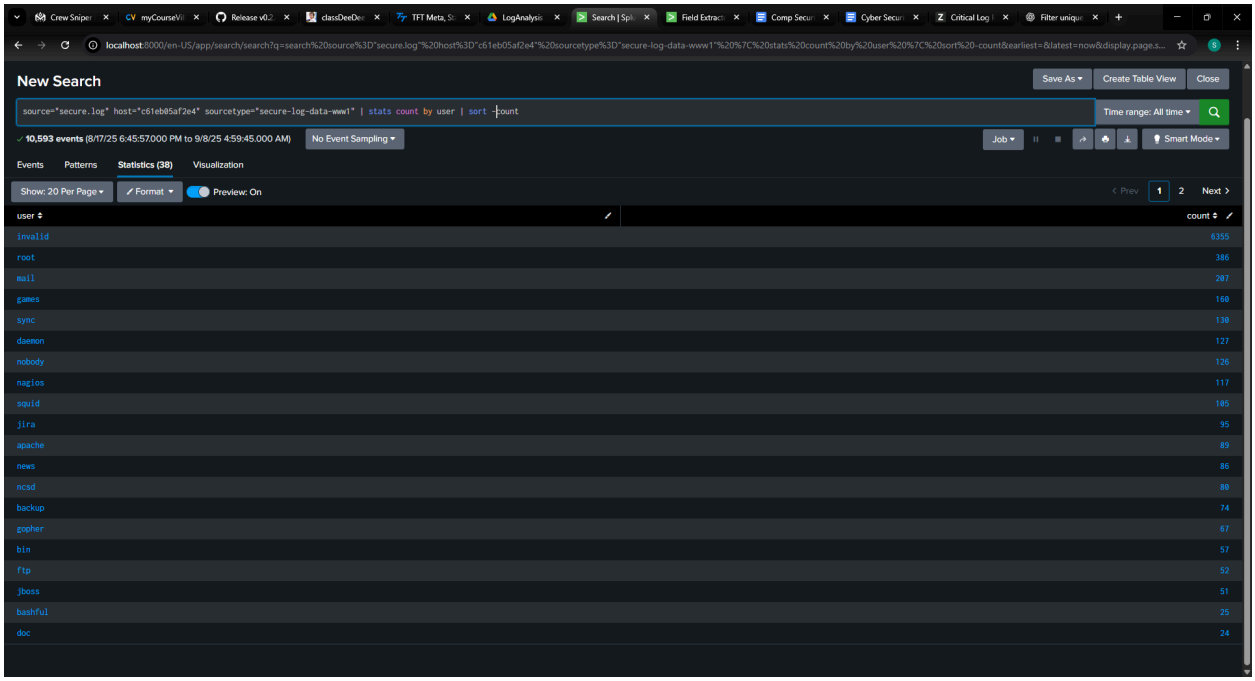
2) What time do hackers appear to try to hack our servers?
Answer The hacker likely set the time to attack at 18:45 the filtered is source="secure.log" host="c61eb05af2e4" sourcetype="Secure-Log-Data-WWW2" | dedup _time | sort _time



3) Which server (mailsv, www1, www2, www3) had the most attempts?
Answer The one with the most attack is www1 with 10,593 (using | stats count)



4) What is the most popular account that hackers use to try to break in?
Answer The most popular one is root (| stats count by user | sort -count)



5) Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?
Answer 299 attempts on passwords.pdf (68 attempts) search.do (70 attempts) show.do (90 attempts) signals.zip(71 attempts). Why are we looking at thess file (.do is an

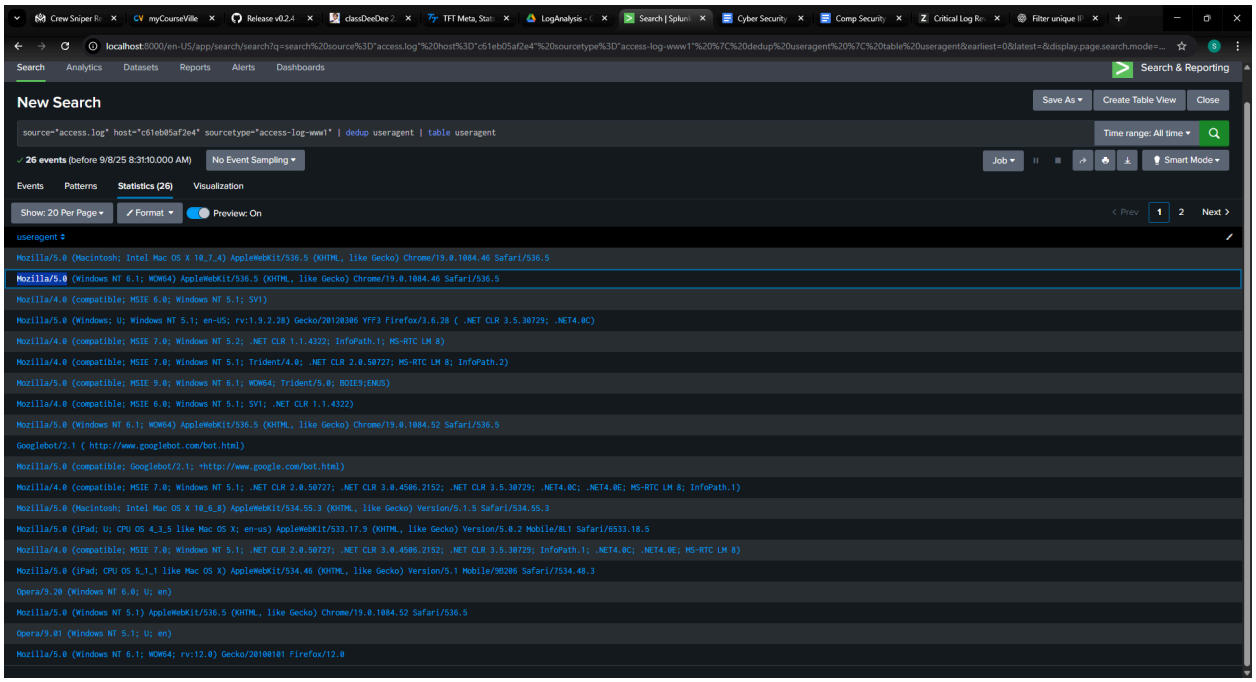
execution command which according to the website this command (show , search etc. is look very out of place for the website)

6) What resource/file are hackers looking for?

Answer According to the name they probably look for passwords file or try to run malicious command on upload (.do file run after it been upload or run on server)

7) Can you find any bots crawling our websites?

Answer yes, there is a bot like Mozzilla/5.0 , Mozilla/4.0, Googlebot/2.1 etc.



8) What are they doing on the site?

Answer it looks like they try to find a vulnerability by accessing multiple possible endpoints by hiding itself by using different sessions and methods.