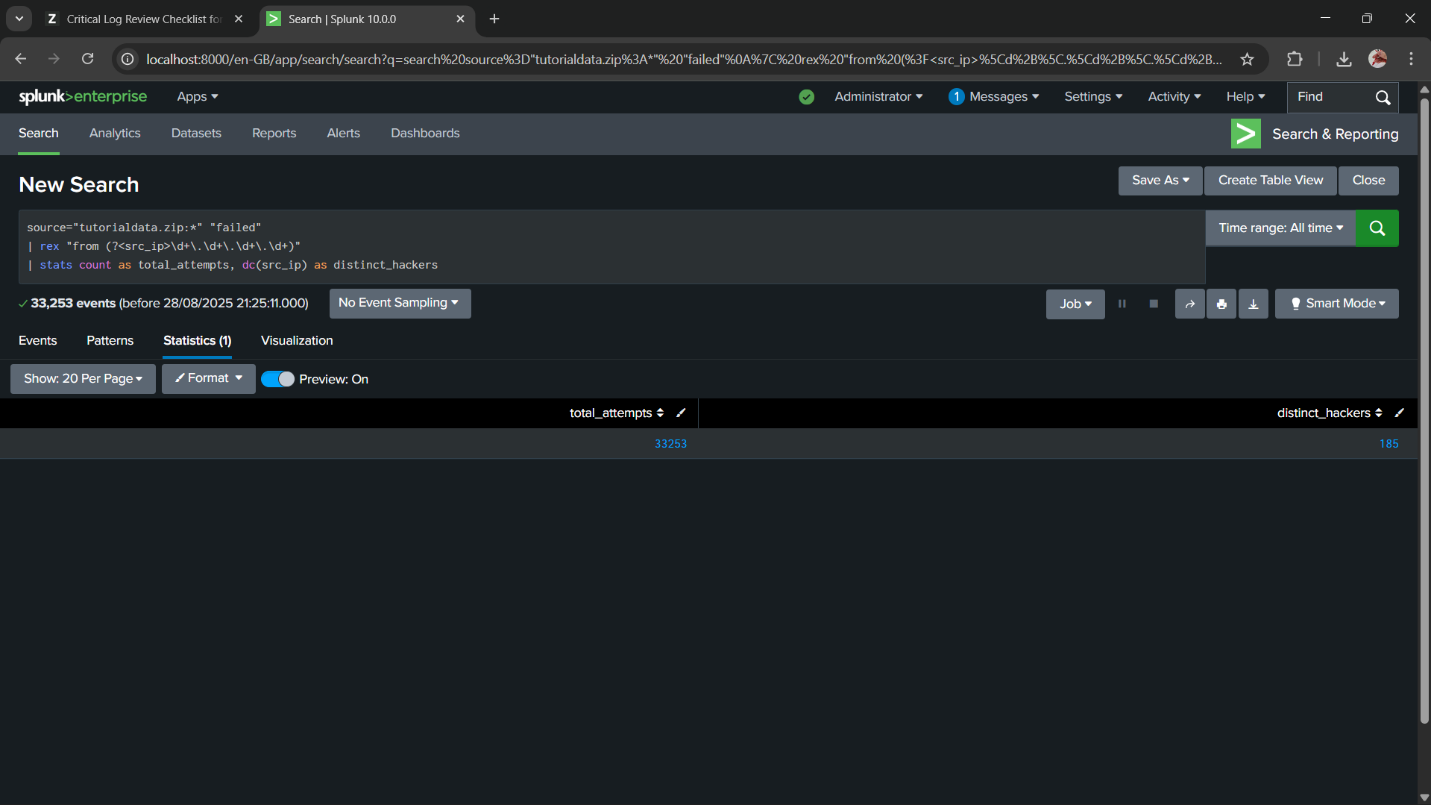
Com Sec Act 2 Splunk

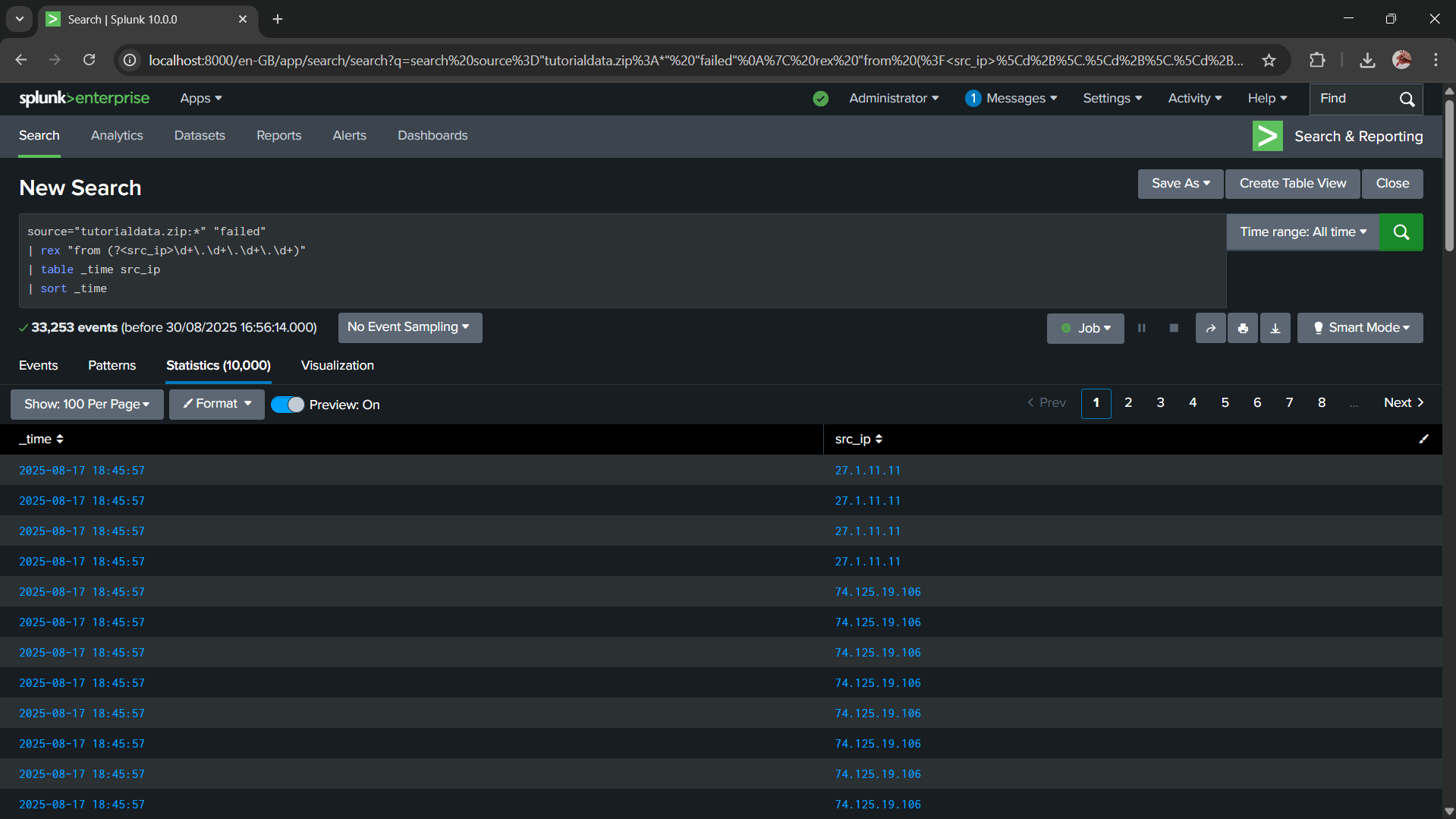
Q1. How many hackers are trying to get access to our servers? And how many

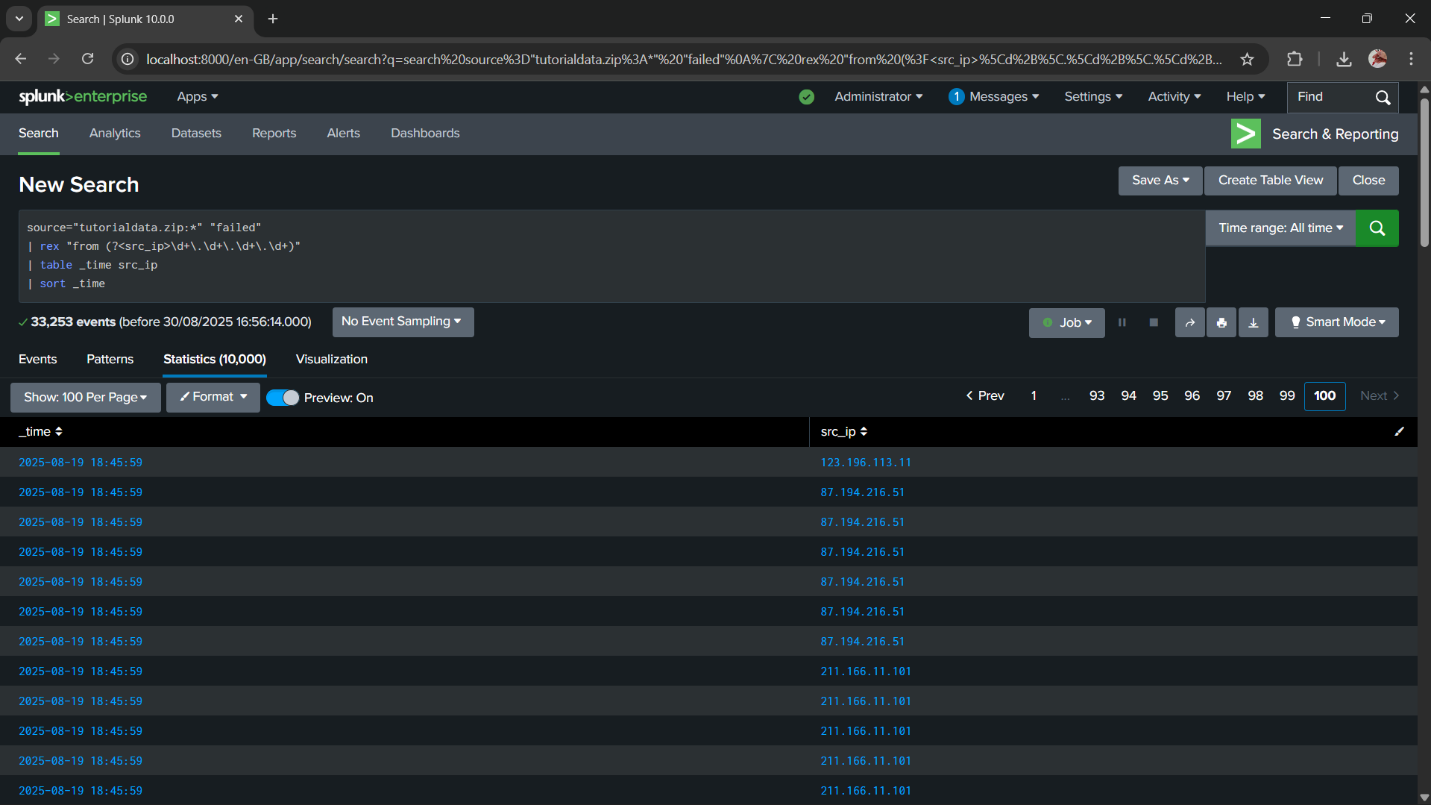
attempts are there? Explain/define how you count distinct hackers.

ANS: #hacker=185, #attempt=33253, We don’t know the actual identity of the hacker, but in log analysis we usually define a distinct hacker by their source IP address.



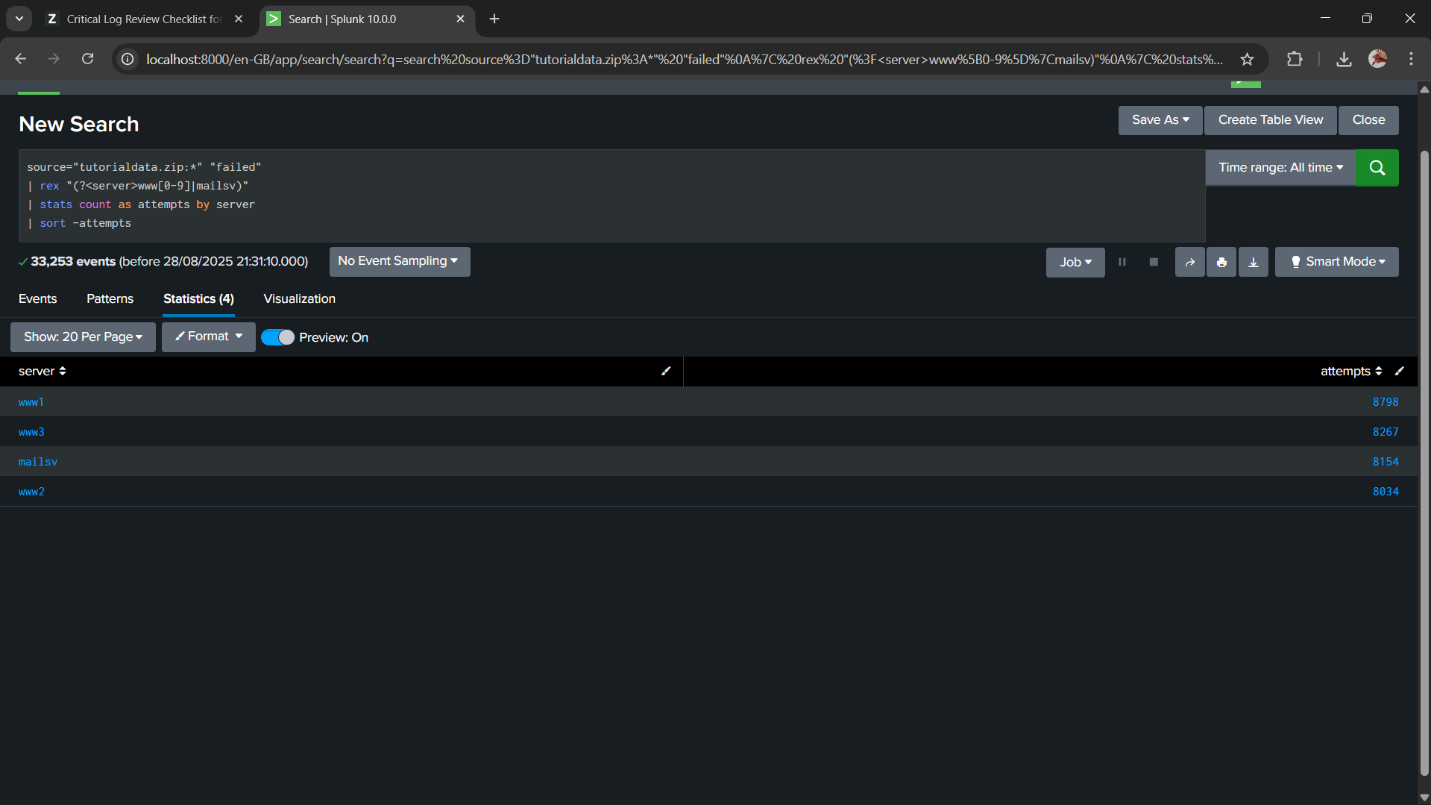
Q2. What time do hackers appear to try to hack our servers?

ANS: many times (ans is in the picture) 



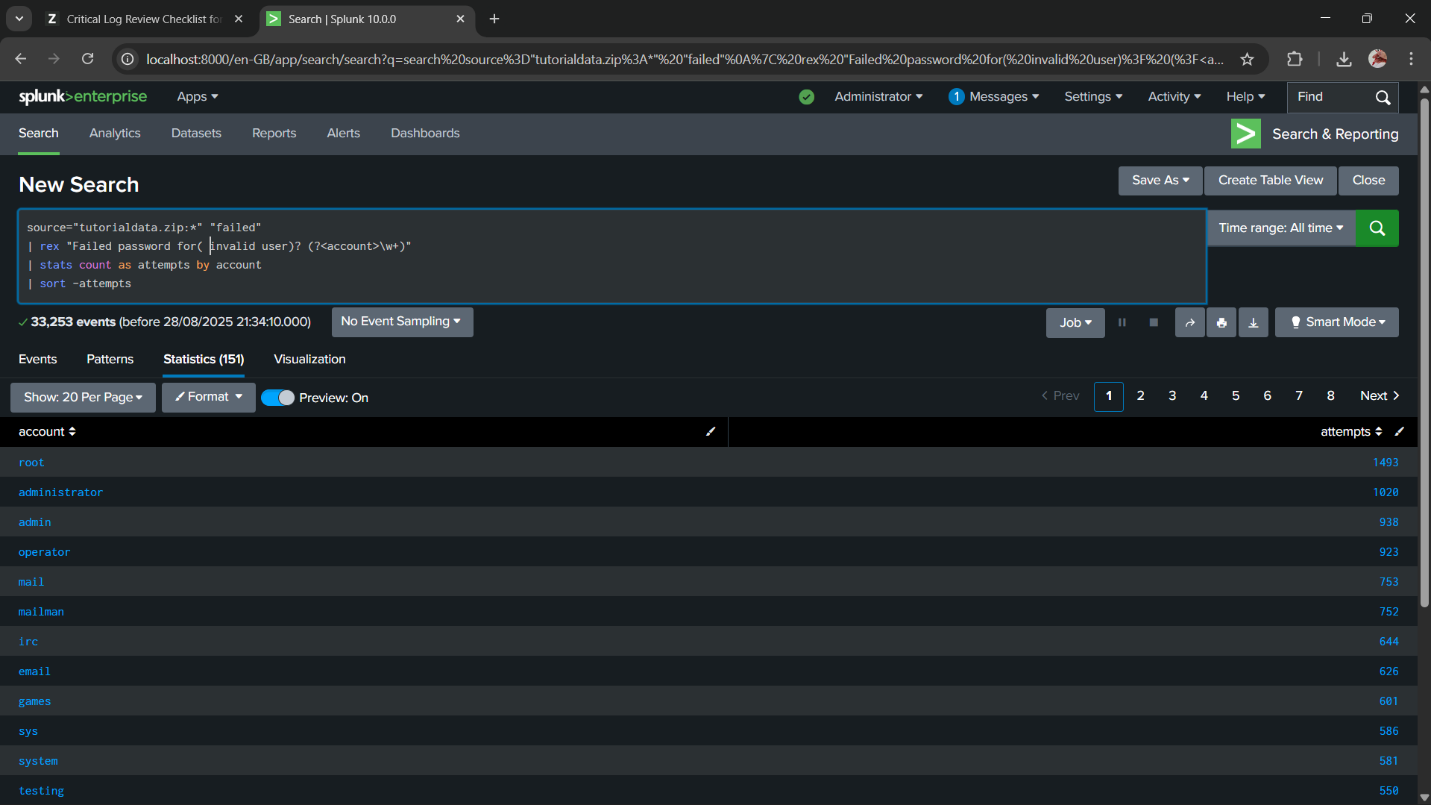
Q3. Which server (mailsv, www1, www2, www3) had the most attempts?

ANS: www1



Q4. What is the most popular account that hackers use to try to break in?

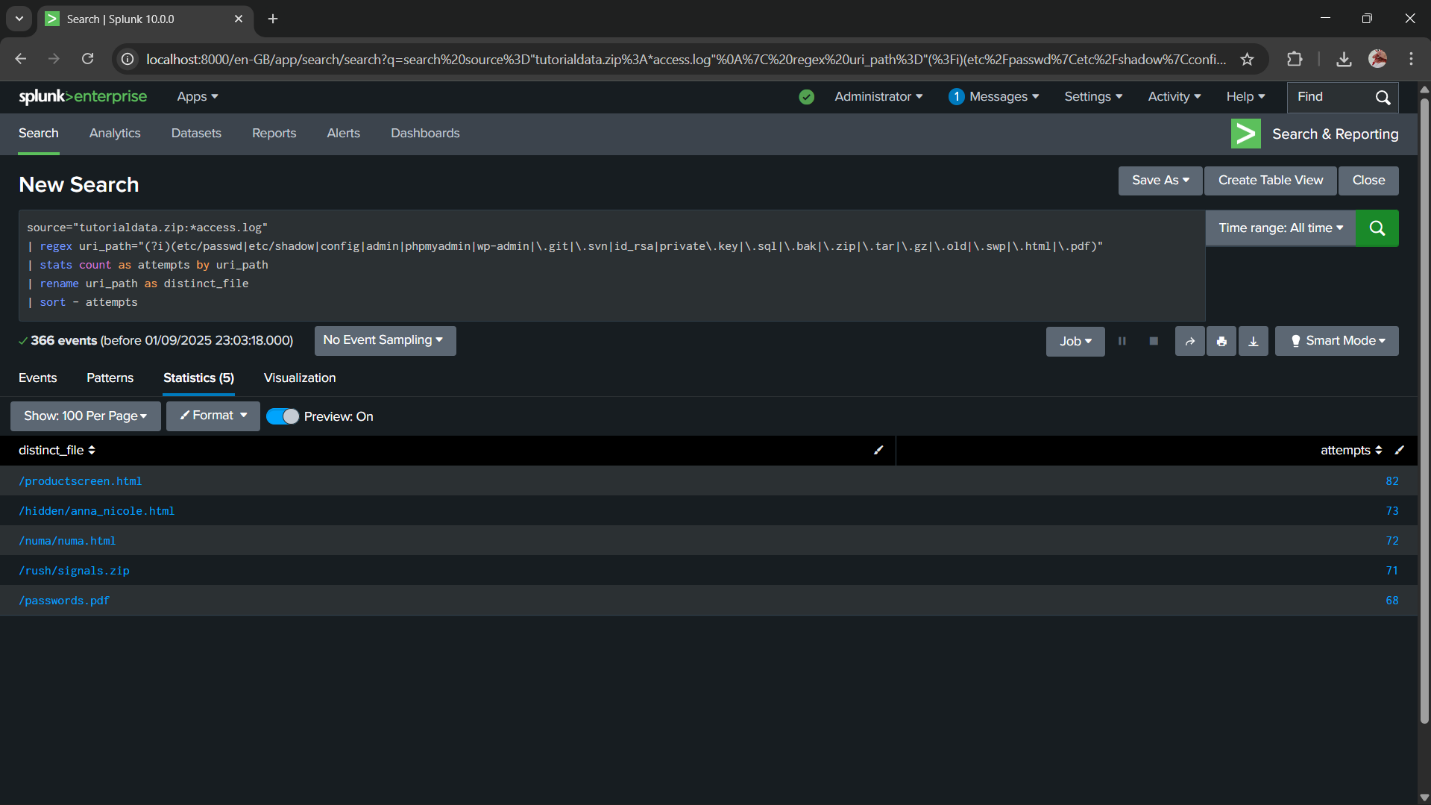
ANS: root



Q5. Can you find attempts to get access to sensitive information from our web

servers? How many attempts were there?

ANS: 366 times

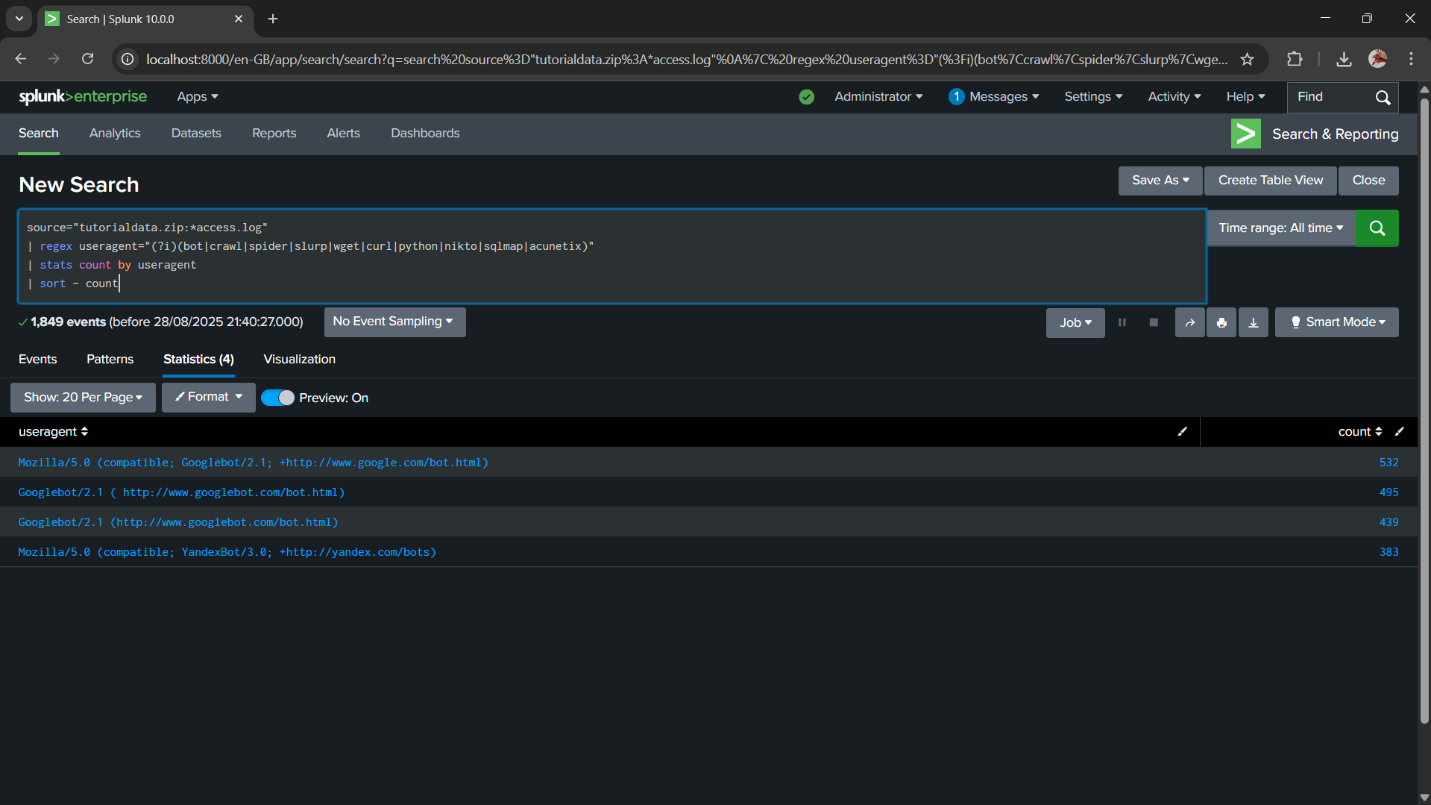


Q6. What resource/file are hackers looking for?

ANS: /productscreen.html, /hidden/anna\_nicole.html, /numa/numa.html, /rush/signals.zip, /password.pdf

Q7. Can you find any bots crawling our websites?

ANS: YES



Q8. What are they doing on the site? (Hint: Look for User-Agent in the web access.logs.)

ANS: Bots are crawling to gain access product, cart, and category pages, the bots are likely:

* **Search engine indexing bots** → to make your site searchable.
* But some crawlers might also be scrapers.

