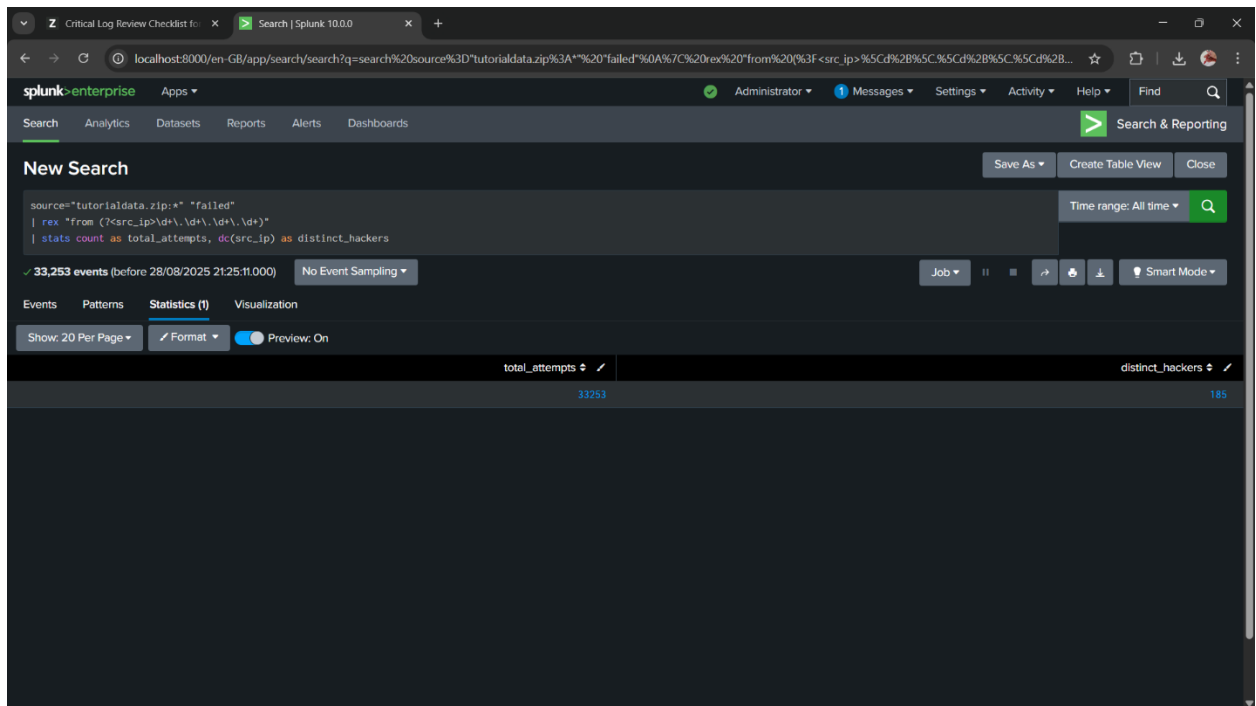


Com Sec Act 2 Splunk

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.



The screenshot shows the Splunk Search interface. The search bar contains the following query:

```
source="tutorialdata.zip:*" "failed"
| rex "from (?<src_ip>[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)"
| stats count as total_attempts, dc(src_ip) as distinct_hackers
```

The search results show 33,253 events (before 28/08/2025 21:25:11.000). The statistics table displays the following data:

total_attempts	distinct_hackers
33253	185

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

ANS: many times (ans is in the picture)

The screenshot shows the Splunk search interface with the following details:

- Search Query:** `source=tutorialdata.zip:* "failed"`
`| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"`
`| table _time src_ip`
`| sort _time`
- Results:** 33,253 events (before 30/08/2025 16:56:14.000). No Event Sampling.
- Table View:** Shows a table with two columns: `_time` and `src_ip`. The first 10 rows are visible, showing timestamps from 2025-08-17 18:45:57 and source IPs like 27.1.11.11 and 74.125.19.106.

The screenshot shows the same Splunk search interface, but with the following details:

- Search Query:** Same as the first screenshot.
- Results:** 33,253 events (before 30/08/2025 16:56:14.000). No Event Sampling.
- Table View:** Shows a table with two columns: `_time` and `src_ip`. The first 10 rows of this view are visible, showing timestamps from 2025-08-19 18:45:59 and source IPs like 123.196.113.11, 87.194.216.51, and 211.166.11.101.

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

ANS: www1

The screenshot shows the Splunk Search interface. The search bar contains the following query:

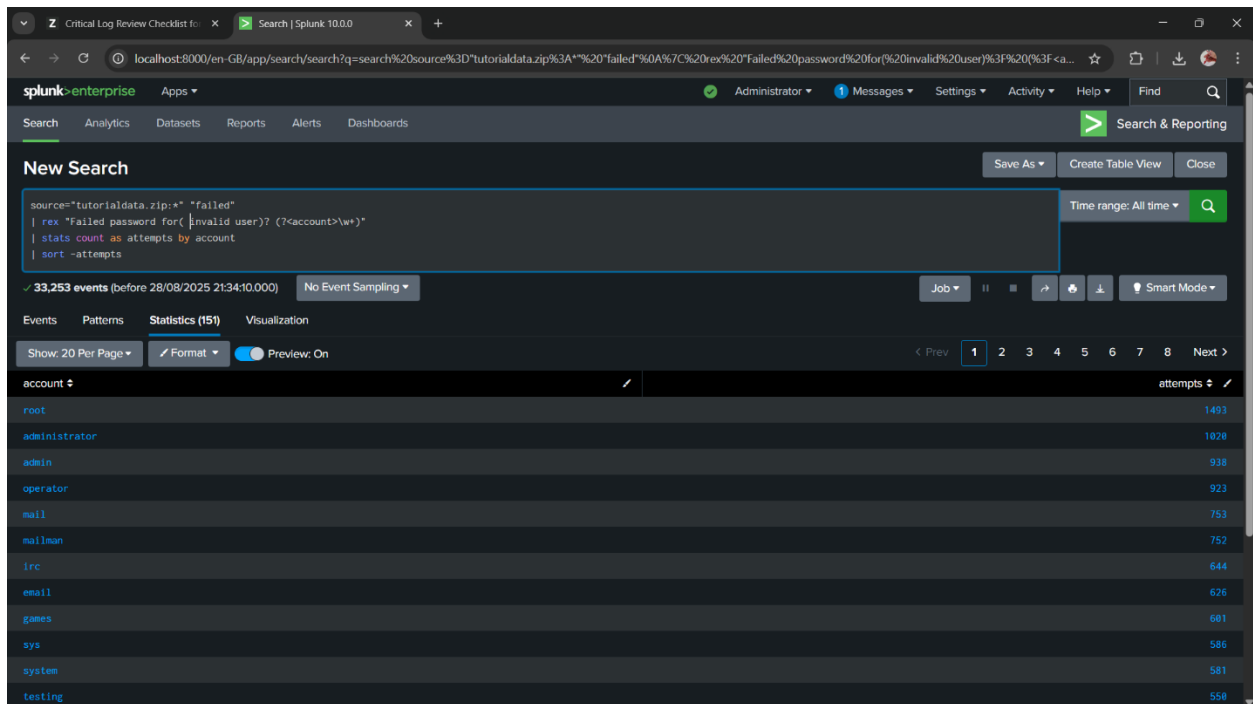
```
source=tutorialdata.zip:* "failed"  
| rex "(?<server>www[0-9])mailsv)"  
| stats count as attempts by server  
| sort -attempts
```

The search results show 33,253 events. The results are displayed in a table with the following columns: server and attempts.

server	attempts
www1	8798
www3	8267
mailsv	8154
www2	8034

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

ANS: root



The screenshot shows the Splunk Enterprise search interface. The search bar contains the following query:

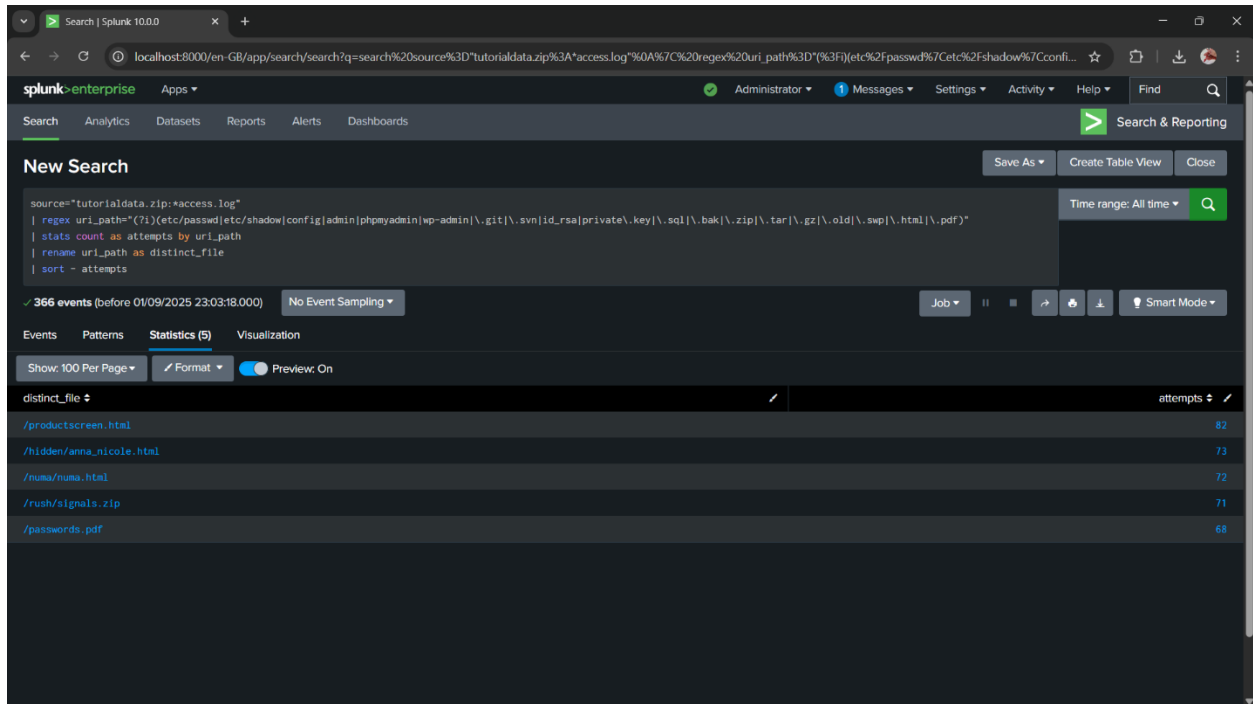
```
source="tutorialdata.zip:*" "failed"
| rex "failed password for(\\invalid user)? (?<account>\\w*)"
| stats count as attempts by account
| sort -attempts
```

The search results are displayed in a table with 15 rows. The table has two columns: 'account' and 'attempts'. The 'root' account has the highest number of attempts (1493).

account	attempts
root	1493
administrator	1028
admin	938
operator	923
mail	753
mailman	752
irc	644
email	626
games	601
sys	586
system	581
testing	550

Q5. Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?

ANS: 366 times



The screenshot shows the Splunk Enterprise interface with a search query: `source="tutorialdata.zip:*access.log" | regex uri_path="(?!)(etc/passwd|etc/shadow|config|admin|phpmyadmin|wp-admin|\.git|\.svn|id_rsa|private|key|\.sql|\.bak|\.zip|\.tar|\.gz|\.old|\.swp|\.html|\.pdf)" | stats count as attempts by uri_path | rename uri_path as distinct_file | sort - attempts`. The results show 366 events, with a table listing the top 5 distinct files and their attempt counts.

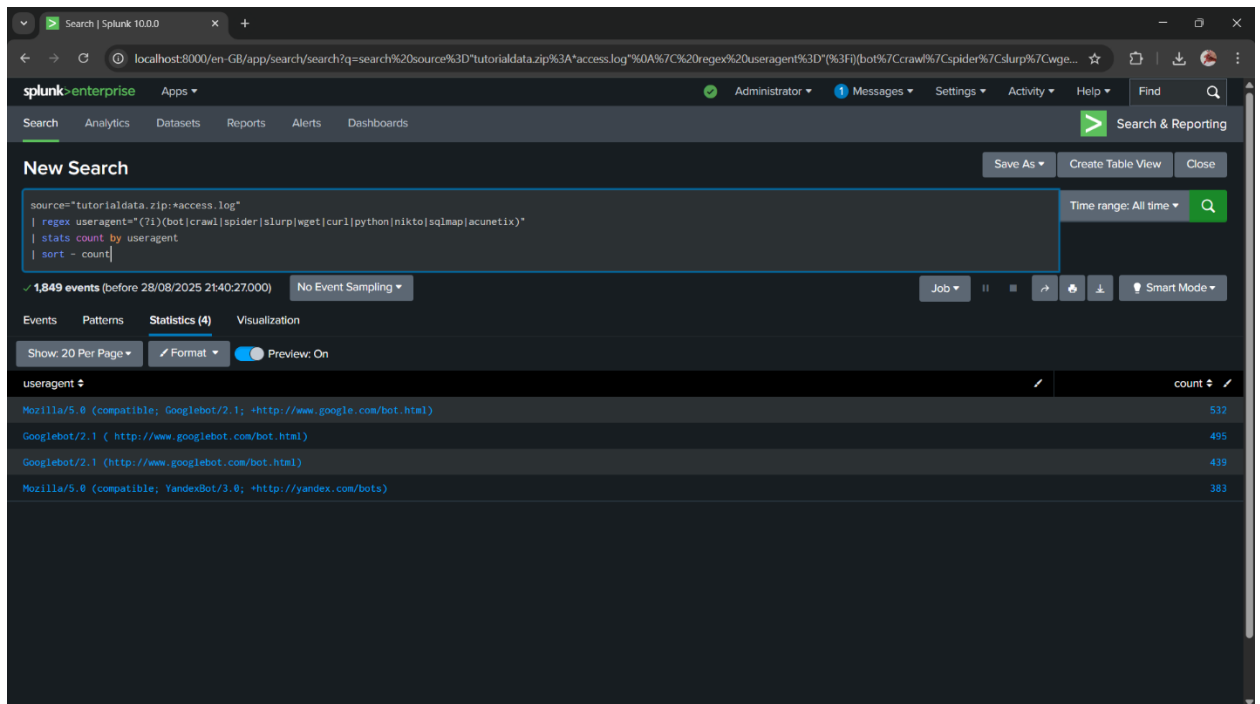
distinct_file	attempts
/productscreen.html	82
/hidden/anna_nicole.html	73
/numa/numa.html	72
/rush/signals.zip	71
/passwords.pdf	68

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



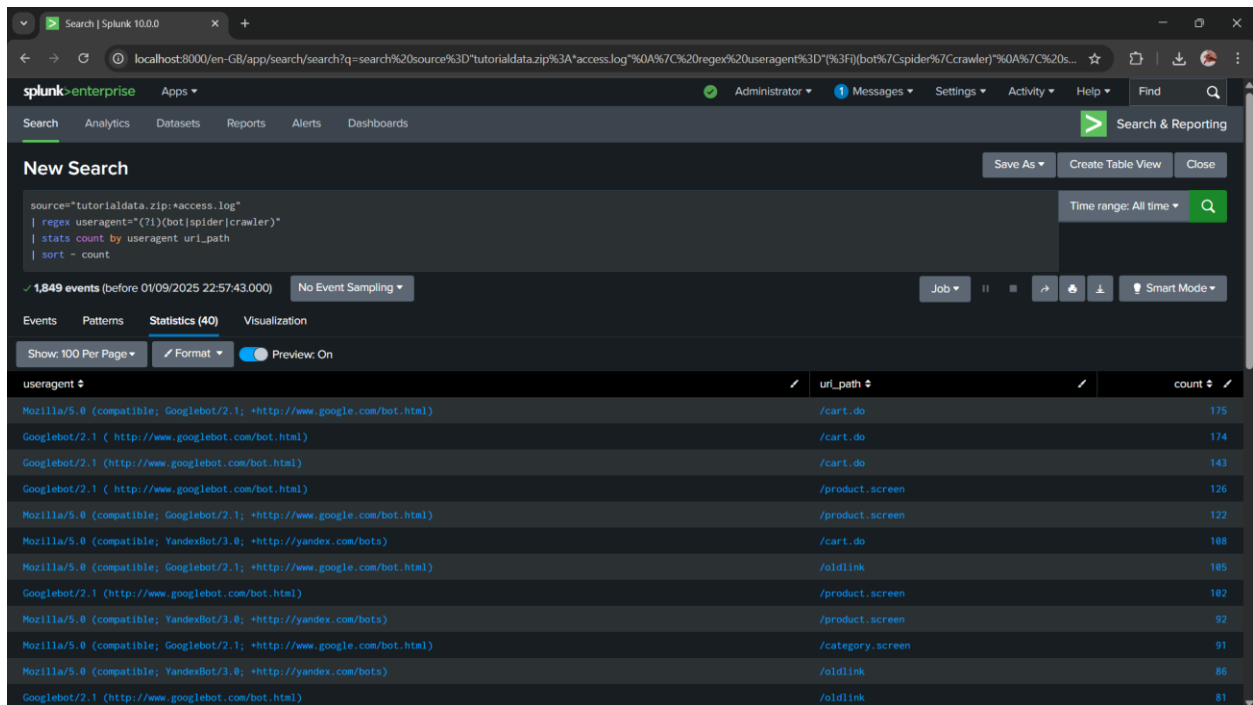
The screenshot shows the Splunk Enterprise interface with a search query that filters for bot useragents. The search results are displayed in a table view, showing the count of events for each useragent. The search query is: `source=tutorialdata.zip:*access.log | regex useragent="(?!)(bot|crawl|spider|slurp|wget|curl|python|nikto|sqlmap|acunetix)" | stats count by useragent | sort - count`. The results show four useragents: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) with 532 events, Googlebot/2.1 (+http://www.googlebot.com/bot.html) with 495 events, Googlebot/2.1 (http://www.googlebot.com/bot.html) with 439 events, and Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) with 383 events.

useragent	count
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	532
Googlebot/2.1 (+http://www.googlebot.com/bot.html)	495
Googlebot/2.1 (http://www.googlebot.com/bot.html)	439
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	383

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.



The screenshot shows the Splunk Search interface. The search query is: `source="tutorialdata.zip:*access.log" | regex useragent="(?!)(bot|spider|crawler)" | stats count by useragent uri_path | sort - count`. The results show 1,849 events. The table below displays the top results, sorted by count.

useragent	uri_path	count
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	/cart.do	175
Googlebot/2.1 (http://www.googlebot.com/bot.html)	/cart.do	174
Googlebot/2.1 (http://www.googlebot.com/bot.html)	/cart.do	143
Googlebot/2.1 (http://www.googlebot.com/bot.html)	/product.screen	126
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	/product.screen	122
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	/cart.do	108
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	/oldlink	105
Googlebot/2.1 (http://www.googlebot.com/bot.html)	/product.screen	102
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	/product.screen	92
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	/category.screen	91
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	/oldlink	86
Googlebot/2.1 (http://www.googlebot.com/bot.html)	/oldlink	81