

Activity : Log Analysis

Part I: Can you find people trying to break into the servers?

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.

Answer 33253 Attempts, 185 Hackers

Splunk Search Command:

Attempts

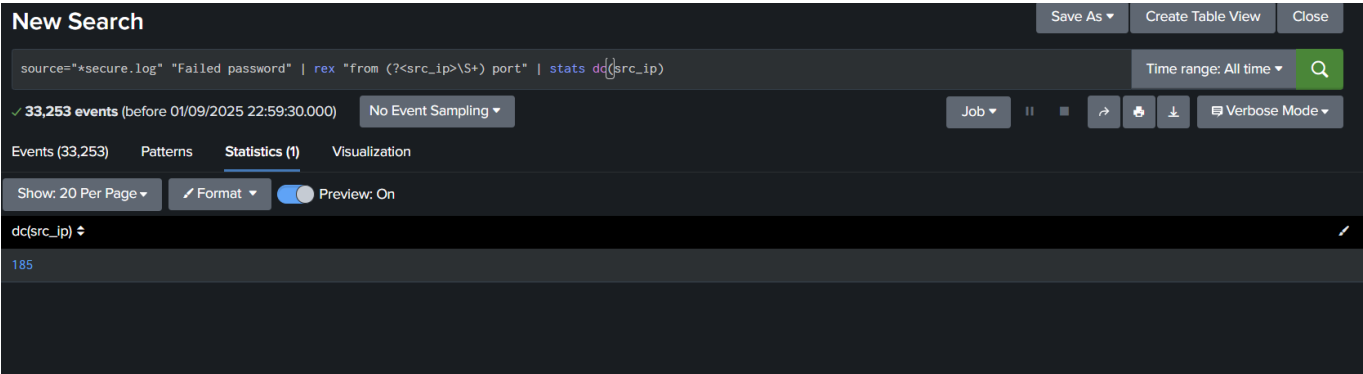
```
source="*secure.log" "Failed password" | stats count
```

The screenshot shows the Splunk Search interface. At the top, the search bar contains the command: `source="*secure.log" "Failed password" | stats count`. Below the search bar, it indicates that 33,253 events were found before 01/09/2025 23:00:17.000. The interface has tabs for Events (33,253), Patterns, Statistics (1), and Visualization. The Statistics tab is selected, showing a table with one row: 'count' with a value of 33253. There are also controls for 'Show: 20 Per Page', 'Format', and a 'Preview: On' toggle.

| count |
|-------|
| 33253 |

Unique Hackers

```
source="*secure.log" "Failed password" | rex "from (?<src_ip>\S+) port" | stats dc(src_ip)
```



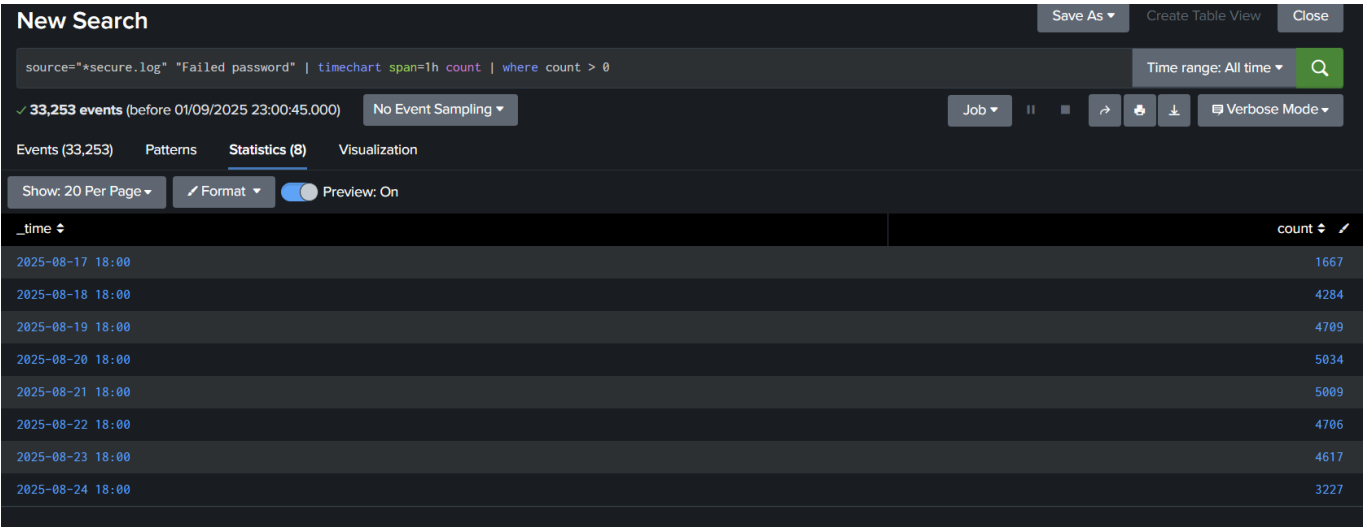
Q2

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

Answer 2025-08-17 to 2025-08-24 at 18:00

Splunk Search Command:

```
source="*secure.log" "Failed password" | timechart span=1h count | where count > 0
```



Results: [Describe the time patterns you observe - peak hours, consistent timing, etc.]

Q3

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

Answer www1

Splunk Search Command:

```
source="*secure.log" "Failed password" | stats count by source
```

The screenshot shows the Splunk Search interface. The search bar contains the query: `source="*secure.log" "Failed password" | stats count by source`. The results show 33,253 events. The search is filtered by time range (All time) and shows 20 results per page. The results table is as follows:

| source | count |
|-------------------------------------|-------|
| tutorialdata.zip:\mailsv\secure.log | 8154 |
| tutorialdata.zip:\www1\secure.log | 8798 |
| tutorialdata.zip:\www2\secure.log | 8034 |
| tutorialdata.zip:\www3\secure.log | 8267 |

Q4

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

Answer Root

Splunk Search Command:

```
source="*secure.log" "Failed password" | rex field=_raw "user (?<username>\w+)" |  
stats count by username | sort -count | head 20
```

splunk>enterpriseApps

SearchAnalyticsDatasetsReportsAlertsDashboards

New Search

source="*secure.log" "Failed password" | rex "for (invalid user)?(?<user>\\$+)" | top user

33,253 events (before 01/09/2025 23:03:29.000)No Event Sampling

Events (33,253)PatternsStatistics (10)Visualization

Show: 20 Per PageFormatPreview: On

| user | count |
|---------------|-------|
| root | 1493 |
| administrator | 1020 |
| admin | 938 |
| operator | 923 |
| mail | 753 |
| mailman | 752 |
| irc | 644 |
| email | 626 |

Part II: Sensitive Files on Web Servers

Q5

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

Answer 742 Attempts with 404 Status,

Splunk Search Commands:

Attempts

```
source="tutorialdata.zip:*/access.log" "404" | stats count
```

New Search

source="tutorialdata.zip:*/access.log" "404" | stats count

✓ 742 events (before 01/09/2025 23:14:37.000)

No Event Sampling ▾

Events (742)

Patterns

Statistics (1)

Visualization

Show: 20 Per Page ▾

✎ Format ▾

☒ Preview: On

count ↕

742

Q6

What resource/file are hackers looking for?

Answer password.pdf, /hidden/anna_nicole.html

Splunk Search Command:

```
source="tutorialdata.zip:*/access.log" "404" | stats count
```

Sensitive Information (find using uri_path)

a itemId 14

a JSESSIONID 100+

linecount 1

a method 2

other 100+

a productId 14

a punct 61

a referer 89

a referer_domain 3

a req_time 100+

a root 5

a splunk_server 1

status 8

timeendpos 7

timestartpos 7

a uri 100+

a uri_path 14

a uri_query 100+

a user 1

a useragent 26

version 1

3 more fields

+ Extract New Fields

L, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 594

host = 127.0.0.1 | source = tutorialdata.zip:\www2\access.log | sourcetype

> 24/08/2025 198.35.1.75 - - [24/Aug/2025:17:19:39] "GET /product.screen?product=11" 200 11 "http://www.buttercupgames.com/category-screen?categoryId=11" 1

uri_path

14 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

| | Count | % |
|--------------------------|-------|---------|
| /product.screen | 96 | 12.938% |
| show.do | 90 | 12.129% |
| /stuff/logo.ico | 84 | 11.321% |
| /productscreen.html | 82 | 11.051% |
| /hidden/anna_nicole.html | 73 | 9.838% |
| /numa/numa.html | 72 | 9.704% |
| /rush/signals.zip | 71 | 9.569% |
| /search.do | 70 | 9.434% |
| /passwords.pdf | 68 | 9.164% |
| /cart.do | 12 | 1.617% |

Part III: Are there bots crawling our websites?

Q7

Can you find any bots crawling our websites?

Answer Googlebot/2.1 (http://www.googlebot.com/bot.html)

Splunk Search Command:

```
source="*access.log" | search useragent="*bot*" | table _time, useragent, file_name
```

New Search

source="*access.log" | search useragent="*bot*" | table _time, useragent, file_name

✓ 1,849 events (before 01/09/2025 23:18:44.000)

No Event Sampling ▾

Events (1,849)

Patterns

Statistics (1,849)

Visualization

Show: 20 Per Page ▾

Format ▾

☒ Preview: On

< P

| _time ↕ | useragent ↕ |
|---------------------|--|
| 2025-08-24 17:50:17 | Googlebot/2.1 (http://www.googlebot.com/bot.html) |
| 2025-08-24 17:48:48 | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| 2025-08-24 17:48:47 | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| 2025-08-24 17:48:47 | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| 2025-08-24 17:48:47 | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |

Q8

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

Answer Indexing for Google search

Splunk Search Command:

```
source="*access.log" useragent="*bot*" | stats count by uri_path, useragent | sort -count
```