

## 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?

Hackers: 185, Attempts: 33253

Command for counting hacker

**New Search**

```
source="tutorialdata (1).zip:.\*/secure.log" failed password | stats distinct_count(ip_address)
```

✓ 33,253 events (before 9/6/20 4:50:08.000 PM) No Event Sampling ▼

Events (33,253) Patterns **Statistics (1)** Visualization

20 Per Page ▼ ↗ Format Preview ▼

distinct\_count(ip\_address) ↕

185

Command for counting attempts

**New Search**

```
source="tutorialdata (1).zip:.\*/secure.log" failed password
```

✓ 33,253 events (before 9/6/20 4:40:35.000 PM) No Event Sampling ▼ Job ▼ ||

Events (33,253) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ ↗ Format 20 Per Page ▼ < Prev 1 2

	i	Time	Event
<b>&lt; Hide Fields</b> :≡ All Fields  SELECTED FIELDS a host 4 a ip_address 100+ a username 100+  INTERESTING FIELDS	>	8/23/20 12:15:05.000 AM	Thu Aug 23 2020 00:15:05 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3768 ssh2 host = mailsv   ip_address = 194.8.74.23   username = appserver
	>	8/23/20 12:15:05.000 AM	Thu Aug 23 2020 00:15:05 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv   ip_address = 194.8.74.23   username = root
	>	8/23/20	Thu Aug 23 2020 00:15:05 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3768 ssh2

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

16-23 Aug 2020 00:15:01

**New Pivot** Save As... Clear Acceleration

✓ 33,253 events (before 9/6/20 4:05:21:000 PM)

Filters: All time

Split Rows: date\_year, date\_month, date\_mday, date\_hour, date\_minute

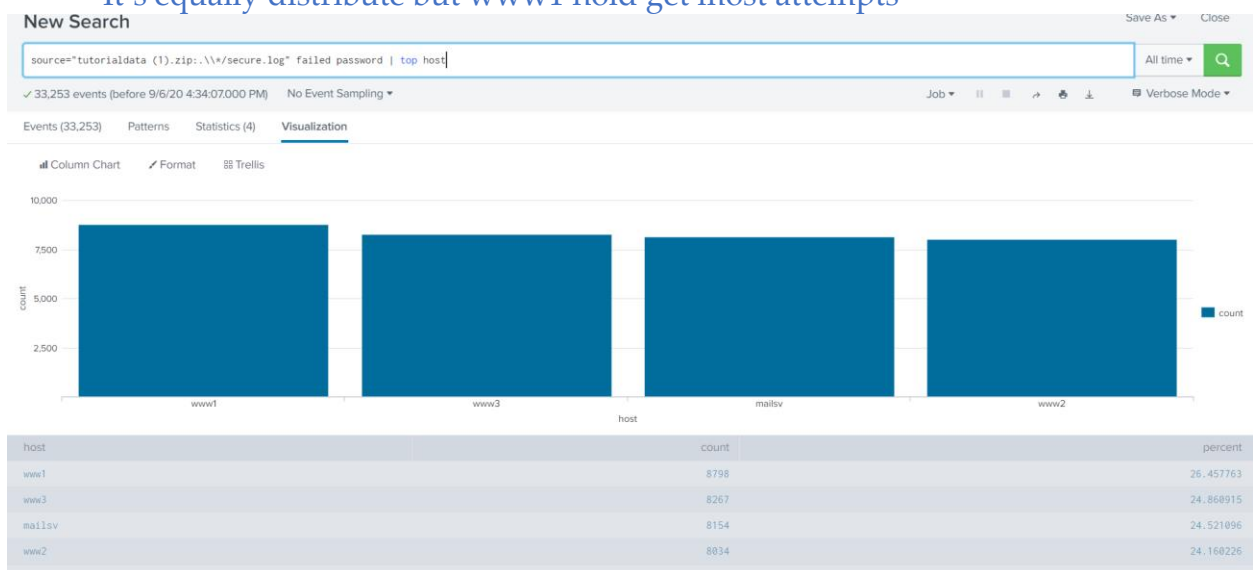
Split Columns: Count of 159...

date_year	date_month	date_mday	date_hour	date_minute	Count of 159382964.679
2020	august	16	0	15	1667
2020	august	17	0	15	4284
2020	august	18	0	15	4709
2020	august	19	0	15	5034
2020	august	20	0	15	5009
2020	august	21	0	15	4706
2020	august	22	0	15	4617
2020	august	23	0	15	3227

This result is visualized from search keyword “failed password”

Q3. Which server (mailsv, www1, www2, www3) seem to see the most attempts?

It’s equally distribute but www1 hold get most attempts

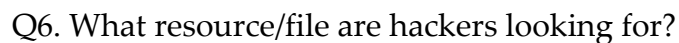


Q4. What is the most popular account that hackers use to try to break in?

The screenshot shows the Splunk Search interface. The search bar contains the query: `source=tutorialdata (1).zip:\\\\v\\secure.log' failed password | stats count by username | sort - count`. The results are displayed as a histogram titled "Visualization". The x-axis is labeled "username" and the y-axis is labeled "count". A tooltip for the "root" username shows a count of 1,493. The histogram shows a long tail of usernames with a single bar for "root" reaching a count of 1,493.

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

Then there are 690 attempts.



List below are resources that they are looking for.

source="tutorialdata (1).zip:.\*\\*/access.log" status=404 | stats count

✓ 690 events (before 9/6/20 6:39:11.000 PM) No Event Sampling ▼

Events (690) Patterns Statistics (1) Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect



List ▼ / Format 20 Per Page ▼

< Hide Fields

≡ All Fields

SELECTED FIELDS

a action 5  
a categoryId 1  
a host 3  
a JSESSIONID 100+  
a productId 2  
# status 1  
a uri 100+  
a uri\_path 9  
a uri\_query 100+  
a user 1

INTERESTING FIELDS

# bytes 100+  
a clientip 100+  
# date\_hour 24  
# date\_mday 8  
# date\_minute 60  
a date\_month 1

uri\_path

9 Values, 100% of events

Reports

Top values

Top values by t

Events with this field

Values

show.do  
/stuff/logo.ico  
/productscreen.html  
/product.screen  
/hidden/anna\_nicole.html  
/numa/numa.html  
/rush/signals.zip  
/search.do  
/passwords.pdf