

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.

New Search Save As Create Table View Close

source="tutorialdata.zip:*\\secure.log" password_status="failed password" (ip="*.*.*.*" OR invalid_user_ip="*.*.*.*") | stats count by ip | where count > 10 All time Q

✓ 33,079 events (before 8/27/23 12:18:46.000 PM) No Event Sampling Job || ↕ ⬆ Smart Mode

Events Patterns **Statistics (185)** Visualization

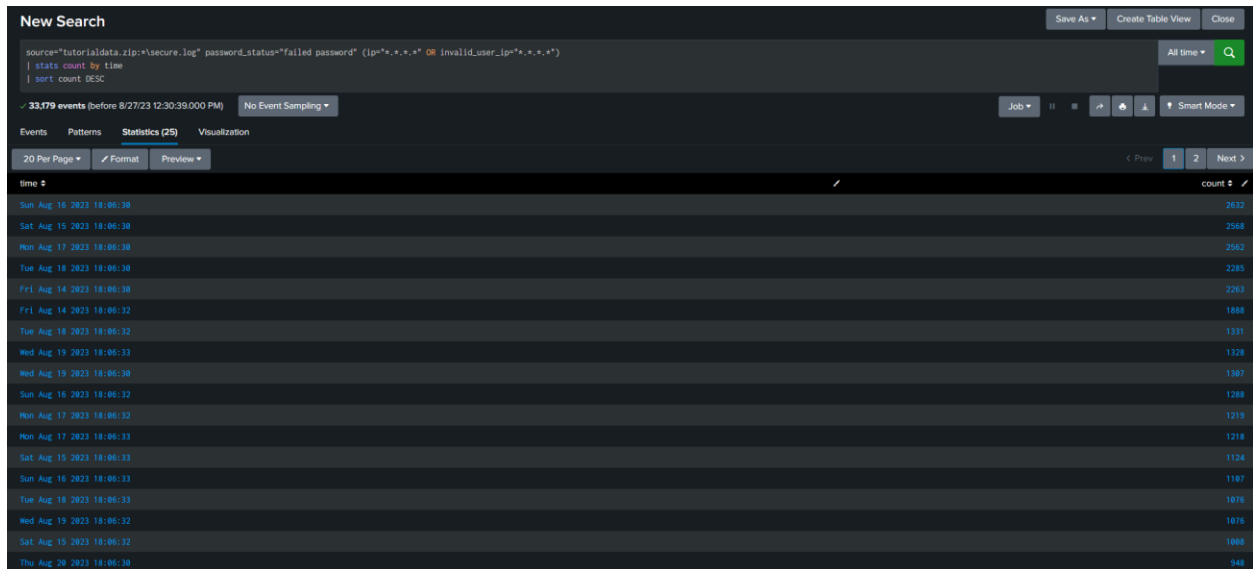
20 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 ... Next >

ip	count
87.194.216.51	257
211.166.11.181	194
138.241.228.82	163
189.169.32.135	142
194.215.285.19	139
18.3.18.46	121
216.221.226.11	183
188.138.40.166	92
187.3.146.287	84
59.162.167.188	84
188.65.113.83	75
65.19.187.94	74
95.138.118.231	74
223.285.219.67	70
59.99.238.91	70
187.231.45.62	68
65.72.161.186	67
173.192.201.242	66
198.228.212.52	65

```
source="tutorialdata.zip:*\\secure.log" password_status="failed
password" (ip="*.*.*.*" OR invalid_user_ip="*.*.*.*")
| stats count by ip
| where count > 10
```

ANS: 185 hackers with 33,179 attempts. Assume that hackers tried more than 10 times to login with any password. So, query status "Failed password" with ip count more than 10 both valid and invalid user.

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

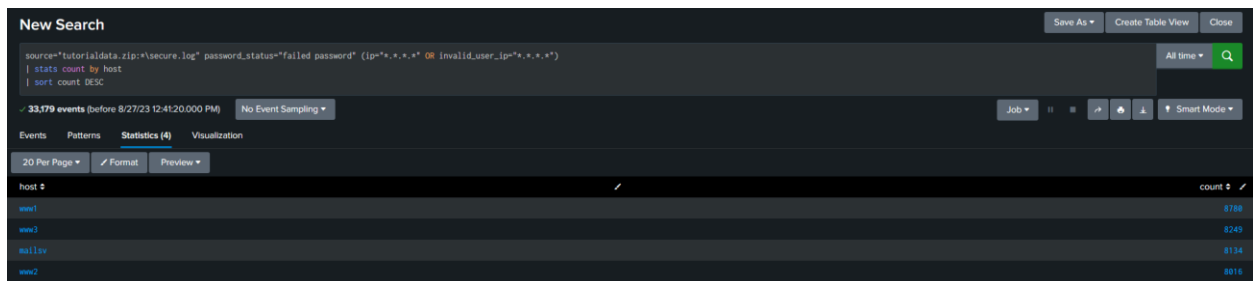


time	count
Sun Aug 16 2023 18:06:30	2632
Sat Aug 15 2023 18:06:30	2568
Mon Aug 17 2023 18:06:30	2552
Tue Aug 18 2023 18:06:30	2285
Fri Aug 14 2023 18:06:30	2263
Fri Aug 14 2023 18:06:32	1888
Tue Aug 18 2023 18:06:32	1331
Wed Aug 19 2023 18:06:33	1328
Wed Aug 19 2023 18:06:38	1387
Sun Aug 16 2023 18:06:32	1288
Mon Aug 17 2023 18:06:32	1219
Mon Aug 17 2023 18:06:33	1218
Sat Aug 15 2023 18:06:33	1124
Sun Aug 16 2023 18:06:33	1187
Tue Aug 18 2023 18:06:33	1076
Wed Aug 19 2023 18:06:32	1076
Sat Aug 15 2023 18:06:32	1068
Thu Aug 28 2023 18:06:38	948

```
source="tutorialdata.zip:*\\secure.log" password_status="failed  
password" (ip="*.\\*.\\*.\\*" OR invalid_user_ip="*.\\*.\\*.\\*")  
| stats count by time  
| sort count DESC
```

ANS: Mostly attempts on "Sun Aug 16 2023 18:06:30"

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



host	count
www1	8780
www3	8245
mailsv	8134
www2	8015

```
source="tutorialdata.zip:*\\secure.log" password_status="failed  
password" (ip="*.\\*.\\*.\\*" OR invalid_user_ip="*.\\*.\\*.\\*")  
| stats count by time  
| sort count DESC
```

ANS: "www1" with 8780 attempts

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

New Search Save As Create Table View Close

```
source="tutorialdata.zip:\secure.log" password_status="failed password" (ip="*.*.*.*" OR invalid_user_ip="*.*.*.*") user!="invalid"
| stats count by user
| sort count DESC
```

9,242 events (before 8/27/23 12:52:58.000 PM) No Event Sampling Job Smart Mode

Events Patterns Statistics (40) Visualization

20 Per Page Format Preview

user	count
root	1493
mail	753
games	681
daemon	528
sync	487
nagios	462
nobody	442
squid	483
apache	336
jira	315
news	312
ncsd	294
backup	282
bin	259
ftp	218
jboss	215
gopher	202
djohnson	121

```
source="tutorialdata.zip:*\\secure.log" password_status="failed
password" (ip="*.*.*.*" OR invalid_user_ip="*.*.*.*")
user!="invalid"

| stats count by user

| sort count DESC
```

ANS: "root" with 1493 attempts

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

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

- Search Bar:** `source=tutorialdata.zip:*access.log" (status="403" OR status="404")`
- Filters:** `| stats count by path`
- Results:** 918 events (before 8/27/23 1:37:10.000 PM), No Event Sampling.
- Table View:** Shows a table with columns 'path' and 'count'.

path	count
/cart.do	56
/category.screen	59
/hidden/anna_nicole.html	73
/numa/numa.html	72
/oldlink	58
/passwords.pdf	68
/product.screen	135
/productscreen.html	82
/rush/signals.zip	71
/search.do	78
/stuff/logo.ico	84
/show.do	98

```
source="tutorialdata.zip:*access.log" (status="403" OR
status="404")
| stats count by path
```

ANS: `"/hidden"` and `"/passwords.pdf"` seems to be the path to the sensitive information. Then query including error status 403 which means URL restriction or error status 404 which means URL not found, sum up within 141 attempts in total.

Q6. What resource/file are hackers looking for?

ANS: `"/hidden/anna_nicole.html"` and `"/passwords.pdf"`

Q7. Can you find any bots crawling our websites?

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

- Search Bar:** `source=tutorialdata.zip:*access.log" useragent="*bot*" | stats count by useragent`
- Filters:** `| stats count by useragent`
- Results:** 1,849 events (before 8/27/23 1:44:36.000 PM), No Event Sampling.
- Table View:** Shows a table with columns 'useragent' and 'count'.

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

```
source="tutorialdata.zip:*access.log" useragent="*bot*"
| stats count by useragent
```

ANS: Yes, as we can see the `"Googlebot"` and `"YandexBot"` from the query above.

Q8. What are they doing on the site?

New Search Save As Create Table View Close

```
source="tutorialdata.zip:*access.log" useragent="*bot*" action="action="
| stats count by action
| sort count DESC
```

600 events (before 8/27/23 2:12:54.000 PM) No Event Sampling Job || ↗ ⬇ Smart Mode

Events Patterns **Statistics (5)** Visualization

20 Per Page Format Preview

action	count
actionaddtocart	223
actionview	153
actionpurchase	143
actionchangequantity	41
actionremove	40

```
source="tutorialdata.zip:*access.log" useragent="*bot*"
action="action="

| stats count by action

| sort count DESC
```

ANS: They mostly "addtocart" with 223 attempts