

Activity 2

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

How many hackers are trying to get access to our servers? -> 185

How many attempts are there? -> 33,253

หาคำตอบได้จาก query ซึ่งจำนวน events ทั้งหมดคือจำนวนครั้ง

New Search

source="tutorialdata.zip:*/secure.log" "Failed password" | stats count by ip | stats dc(ip) as distinct_ip_count

✓ 33,253 events (before 8/26/24 6:33:07.000 AM)

No Event Sampling ▾

Events

Patterns

Statistics (1)

Visualization

20 Per Page ▾

Format

Preview ▾

distinct_ip_count ⇅

185

New Search

Save As ▾

Create Table View

Close

source="tutorialdata.zip:*/secure.log" "Failed password" | stats values(user) as users, count as attempts by ip | sort - attempts

All time ▾

Q

✓ 33,253 events (before 8/26/24 6:38:30.000 AM)

No Event Sampling ▾

Job ▾

II

▀

↶

↷

↓

Policy-Based Pool ▾

Smart Mode ▾

Events

Patterns

Statistics (185)

Visualization

20 Per Page ▾

Format

Preview ▾

< Prev

1

2

3

4

5

6

7

8

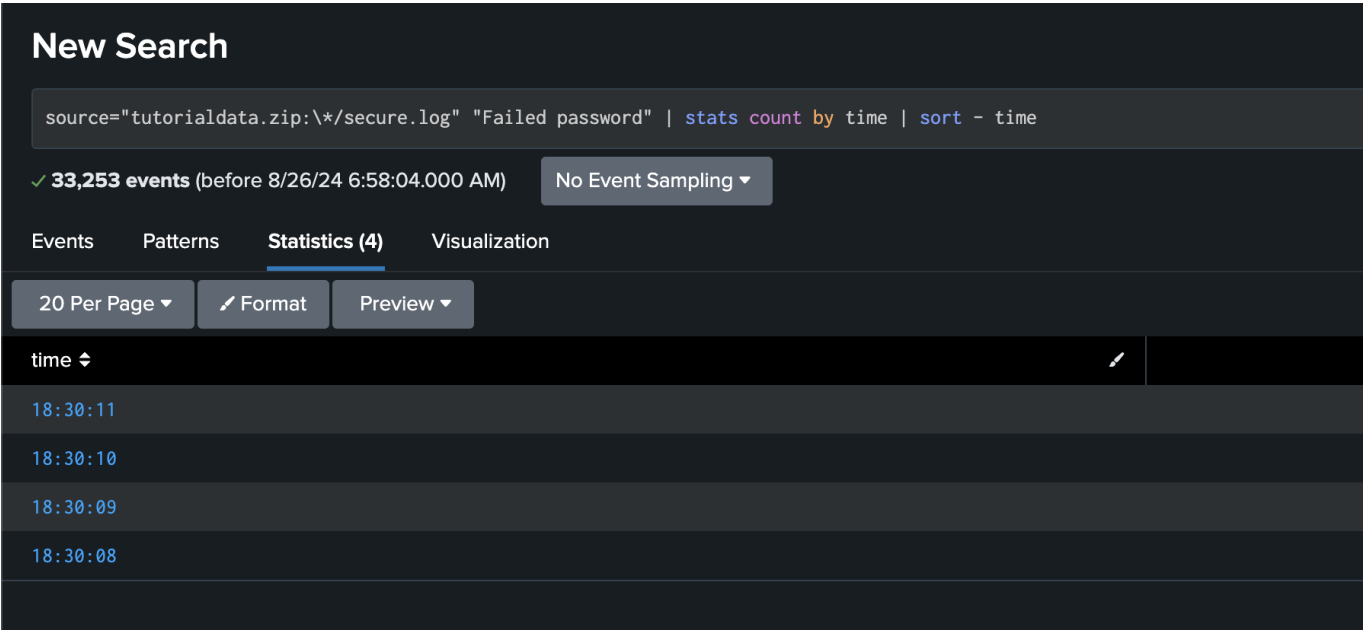
...

Next >

ip ⇅	users ⇅	attempts ⇅
87.194.216.51		257
211.166.11.101		194
128.241.220.82		163
109.169.32.135		142
194.215.205.19		139
10.3.10.46		121
216.221.226.11		103
188.138.40.166		92

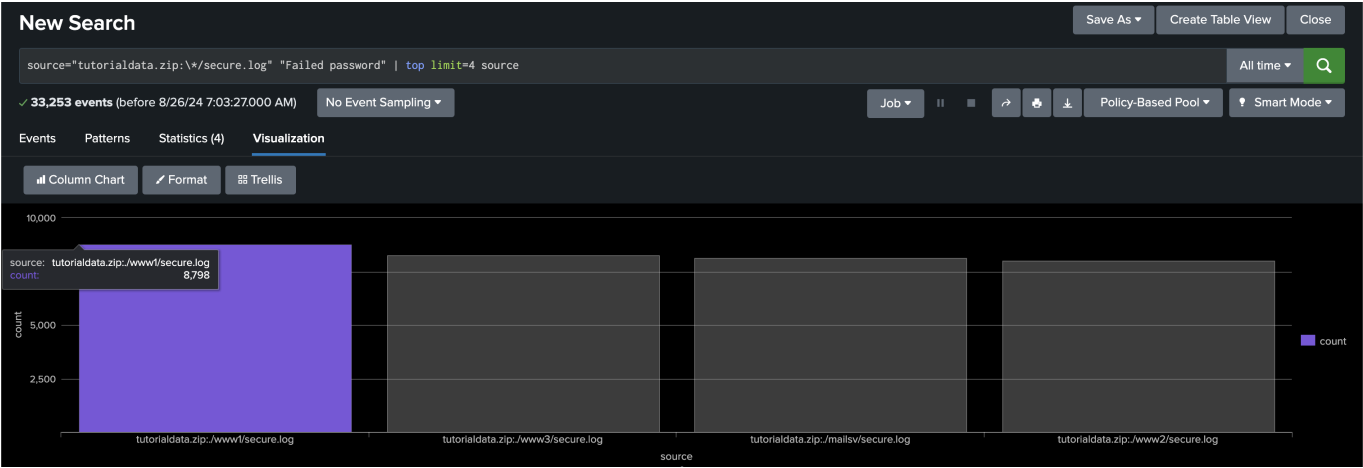
Q2. What time do hackers appear to try to hack our servers?

Ans 18:30:08 - 18:30:11



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

Ans www1 วิธีการหาคำตอบมาจากการใช้ Query ด้านล่าง ซึ่งจะแสดงให้เห็นว่าการโจมตีส่วนใหญ่พุ่งเป้าไปที่ www1 โดยในกรณีนี้ เราถือว่าจำนวนผู้ใช้งานที่ไม่ใช่ Hacker มีจำนวนครั้งในการใช้งานน้อยมาก จนสามารถละเว้นไปได้



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

Ans root โดยตรงลงมาคือ administrator, admin, operator ตามลำดับ

New Search

Save As>Create Table View>Close

source="tutorialdata.zip:*/secure.log" "Failed password" | rex "Failed password for (invalid user)?(?<account>\w*)" | stats count by account | sort - count

All time>Q

✓33,253 events (before 8/26/24 5:42:05.000 AM)No Event Sampling

Job>||■↶↷⬇️Policy-Based Pool>Smart Mode>

EventsPatternsStatistics (151)Visualization

20 Per Page>FormatPreview>

< Prev12345678Next>

account	count
root	1493
administrator	1020
admin	938
operator	923
mail	753
mailman	752

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

Ans

1. ทำการ query และ count จำนวน status ทั้งหมด

New Search

Save As>Create Table View>Close

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

All time>Q

✓39,532 events (before 8/26/24 8:46:40.000 AM)No Event Sampling

Job>||■↶↷⬇️Policy-Based Pool>Smart Mode>

EventsPatternsStatistics (9)Visualization

20 Per Page>FormatPreview>

status	count
200	34282
400	701
403	228
404	690
406	710
408	756
500	733
503	952
505	480

2. ทำการหาผลรวมของ status 401, 403, 400, 500 (เนื่องจาก user ทั่วไปมีโอกาสได้รับ status code นี้น้อยมาก จึง assume ว่าเป็น status code ของ hacker ทั้งหมด)

New Search

```
source="tutorialdata.zip:*/access.log"
| stats count by status
| where status IN (401, 403, 400, 500)
| stats sum(count) as total_errors
```

✓ **39,532 events** (before 8/26/24 8:50:53.000 AM) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

total_errors ↕

1662

1662

Q6. What resource/file are hackers looking for?

Ans ทำการ query จาก url path โดยสนใจแค่ status code ที่น่าสงสัยเท่านั้น ซึ่งได้ผลลัพธ์ดังนี้

New Search

```
source="tutorialdata.zip:*/access.log"
| rex "(?<captured_url_path>/\S+)\?"
| rex "(?<captured_url_path>[^/\s]+)\?"
| where status IN (401, 403, 400, 500, 404)
| stats count by captured_url_path
```

✓ **2,352 events** (before 8/26/24 8:54:00.000 AM) No Event Sampling ▼ Job ▼ || ↶ ↷ ⬇ Policy-Based Pool ▼ Smart Mode ▼

Events Patterns **Statistics (12)** Visualization

20 Per Page ▼ Format Preview ▼

captured_url_path ↕	count ↕
anna_nicole.html	73
cart.do	428
category.screen	374
logo.ico	84
numa.html	72
oldlink	415
passwords.pdf	68
product.screen	525
productscreen.html	82
search.do	70
show.do	90
signals.zip	71

Q7. Can you find any bots crawling our websites?

Ans

1. ทำการ search คำว่า bot เพื่อดูตัวอย่างของ log ที่มี bot
2. ทำการ filter โดย extract field และ count field

New Search [Save As] [Create Table View] [Close]

Source="tutorialdata.zip:./*/access.log"
| search bot="*bot*" OR bot="*Bot*" | stats count by bot [All time] [Q]

✓ 915 events (before 8/26/24 8:46:30.000 AM) [No Event Sampling] [Job] [Pause] [Refresh] [Download] [Policy-Based Pool] [Smart Mode]

Events Patterns **Statistics (2)** Visualization

20 Per Page [Format] [Preview]

bot	count
compatible; Googlebot/2.1	532
compatible; YandexBot/3.0	383

จะเห็นได้ว่ามี 2 bot คือ **Googlebot/2.1** และ **YandexBot/3.0**

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

Ans Googlebot/2.1 และ YandexBot/3.0 เป็นบอทจากเครื่องมือค้นหาที่ทำหน้าที่เก็บข้อมูลเว็บไซต์เพื่อปรับปรุงผลการค้นหา การเข้าถึงของพวกเขาก็จะถูกบันทึกในล็อกการเข้าถึง ภายใต้ฟิลด์ User-Agent โดยพวกเขาจะรวบรวมข้อมูลหน้าเว็บเพื่อใช้ในการจัดอันดับในผลการค้นหา