

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.

Ans 185 people and 66,506 attempts, counted from events where the password failed more than 10 times.

```
source="tutorialdata.zip:./secure.log" "Failed password"
| rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip
| where count > 10
```

| New Search | | Save As ▾ | Create Table View | Close |
|--|--|-----------------------------------|-------------------|----------------|
| source="tutorialdata.zip:./secure.log" "Failed password" rex "from (?<ip>\d+\.\d+\.\d+\.\d+)" stats count by ip where count > 10 | | All time ▾ | Q | |
| ✓ 66,506 events (before 20/08/2024 14:20:27.000) No Event Sampling ▾ | | Job ▾ | | Verbose Mode ▾ |
| Events (66,506) Patterns Statistics (185) Visualization | | | | |
| 20 Per Page ▾ Format Preview ▾ | | < Prev 1 2 3 4 5 6 7 8 ... Next > | | |
| ip ↕ | | count ↕ | | |
| 10.1.10.172 | | 32 | | |
| 10.2.10.163 | | 94 | | |
| 10.3.10.46 | | 242 | | |
| 107.3.146.207 | | 564 | | |
| 108.65.113.83 | | 498 | | |
| 109.169.32.135 | | 1030 | | |

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

Ans 18:30

```
source="tutorialdata.zip:./secure.log" "Failed password"
| rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
| bin span=1m _time
| stats count by _time, ip
| where count > 10
| table _time, ip | join ip [
  search source="tutorialdata.zip:./secure.log" "Failed password"
  | rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
  | bin span=1m _time
  | stats count by _time, ip ]
```

New Search Save As Create Table View Close

```
source="tutorialdata.zip:.*/*secure.log" "Failed password"
| rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
| bin span=1m _time
| stats count by _time, ip
| where count > 10
| table _time, ip
| join ip [
  search source="tutorialdata.zip:.*/*secure.log" "Failed password"
  | rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
  | bin span=1m _time
  | stats count by _time, ip
]
```

✓ 99,759 events (before 20/08/2024 15:01:54.000) No Event Sampling

Events (99,759) Patterns **Statistics (1185)** Visualization

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

| _time | ip | count |
|---------------------|-----------------|-------|
| 2024-08-11 18:30:00 | 10.3.10.46 | 18 |
| 2024-08-11 18:30:00 | 110.138.30.229 | 99 |
| 2024-08-11 18:30:00 | 110.159.208.78 | 60 |
| 2024-08-11 18:30:00 | 111.161.27.20 | 12 |
| 2024-08-11 18:30:00 | 118.142.68.222 | 72 |
| 2024-08-11 18:30:00 | 124.160.192.241 | 48 |
| 2024-08-11 18:30:00 | 125.7.55.180 | 15 |

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

Ans www1

source="tutorialdata.zip:.*/*secure.log" "Failed password" | top source | head 1

New Search Save As Create Table View Close

source="tutorialdata.zip:.*/*secure.log" "Failed password" | top source | head 1 All time Q

✓ 99,759 events (before 20/08/2024 15:21:17.000) No Event Sampling

Events (99,759) Patterns **Statistics (1)** Visualization

100 Per Page Format Preview

| source | count | percent |
|---|-------|-----------|
| tutorialdata.zip:./tutorialdata/www1/secure.log | 26394 | 26.457763 |

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

Ans root

source="tutorialdata.zip:.*/*secure.log" "Failed password" NOT "invalid user"
 | rex "for (?<account>\w+)"
 | stats count by account

```
| sort - count
| table account, count
| head 1
```

New Search

source="tutorialdata.zip:.*secure.log" "Failed password" NOT "invalid user"
| rex "for (?>account>\\w+)"
| stats count by account
| sort - count
| table account, count | head 1

27,726 events (before 20/08/2024 15:18:50.000) No Event Sampling

Events (27,726) Patterns Statistics (1) Visualization

100 Per Page Format Preview

| account | count |
|---------|-------|
| root | 4479 |

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?

Ans Yes, after reviewing the web server's access logs, I found 9,408 attempts to access sensitive information. These were flagged by filtering for HTTP status codes like 401 (Unauthorized), 403 (Forbidden), 404 (Not Found), and 500 (Internal Server Error), which often indicate unauthorized access attempts or suspicious activity.

```
source="tutorialdata.zip:.*access.log" status=400 OR status=401 OR status=403 OR status=404 OR status=500
| stats count by status
```

New Search

source="tutorialdata.zip:.*access.log" status=400 OR status=401 OR status=403 OR status=404 OR status=500
| stats count by status

9,408 events (before 25/08/2024 05:20:40.000) No Event Sampling

Events (9,408) Patterns Statistics (4) Visualization

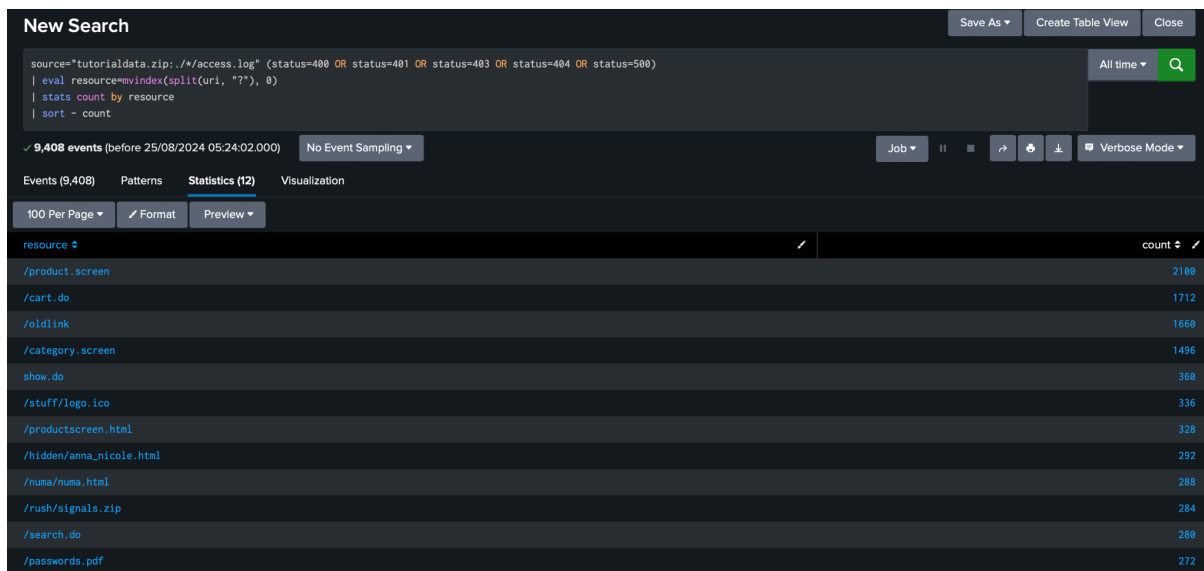
100 Per Page Format Preview

| status | count |
|--------|-------|
| 400 | 2884 |
| 403 | 912 |
| 404 | 2768 |
| 500 | 2932 |

Q6. What resource/file are hackers looking for?

Ans The files in the image below are the ones the hacker is likely looking for, based on the status codes.

```
source="tutorialdata.zip:./*/access.log" (status=400 OR status=401 OR status=403  
OR status=404 OR status=500)  
| eval resource=mindex(split(uri, "?"), 0)  
| stats count by resource  
| sort - count
```



The screenshot shows the Splunk Search interface with the following search query:

```
source="tutorialdata.zip:./*/access.log" (status=400 OR status=401 OR status=403 OR status=404 OR status=500)  
| eval resource=mindex(split(uri, "?"), 0)  
| stats count by resource  
| sort - count
```

The search results are displayed in a table with 12 columns. The first column is 'resource' and the second column is 'count'. The results are sorted by count in descending order.

| resource | count |
|--------------------------|-------|
| /product.screen | 2100 |
| /cart.do | 1712 |
| /oldlink | 1668 |
| /category.screen | 1496 |
| show.do | 368 |
| /stuff/logo.ico | 336 |
| /productscreen.html | 328 |
| /hidden/anna_nicole.html | 292 |
| /numa/numa.html | 288 |
| /rush/signals.zip | 284 |
| /search.do | 280 |
| /passwords.pdf | 272 |

Part III. Are there bots crawling our websites?

Q7. Can you find any bots crawling our websites?

Ans Yes, I found **Mozilla/5.0** and **Googlebot/2.1** after filtering the user agents for terms like **bot**, **crawler**, **spider**, **slurp**, **archive**, and **scanner**.

```
source="tutorialdata.zip:./*/access.log"  
| stats count by useragent  
| search useragent IN ("*bot*", "*crawler*", "*spider*", "*slurp*", "*archive*",  
"*scanner*")  
| sort -count
```

New Search

Save As

Create Table View

Close

```
source="tutorialdata.zip:./*/access.log"
| stats count by useragent
| search useragent IN ("*bot*", "*crawler*", "*spider*", "*slurp*", "*archive*", "*scanner*")
| sort -count
```

All time

Q

7,396 events (before 25/08/2024 05:35:40.000)

No Event Sampling

Job

II

Verbose Mode

Events (7,396)

Patterns

Statistics (4)

Visualization

100 Per Page

Format

Preview

| useragent | count |
|--|-------|
| Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 2128 |
| Googlebot/2.1 (http://www.googlebot.com/bot.html) | 1988 |
| Googlebot/2.1 (http://www.googlebot.com/bot.html) | 1756 |
| Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) | 1532 |

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

Ans The bots, specifically Googlebot/2.1 and YandexBot/3.0, are crawling various parts of the site to index its content for search engines like Google and Yandex. They're accessing pages like /cart.do, /product.screen, and /category.screen, as well as some older links and specific files. This activity helps ensure that these pages and files are included in search results, making them easier for users to find online.

```
source="tutorialdata.zip:./*/access.log"
| search useragent IN ("*bot*", "*crawler*", "*spider*", "*slurp*", "*archive*",
"*scanner*")
| eval resource=mvindex(split(uri, "?"), 0)
| stats count by resource, useragent
| sort - count
```

New Search

Save As

Create Table View

Close

```
source="tutorialdata.zip:./*/access.log"
| search useragent IN ("*bot*", "*crawler*", "*spider*", "*slurp*", "*archive*", "*scanners*")
| eval resource=mvindex(split(uri, "?"), 0)
| stats count by resource, useragent
| sort - count
```

All time

Q

7,396 events (before 25/08/2024 05:50:29.000)

No Event Sampling

Job

II

Verbose Mode

Events (7,396)

Patterns

Statistics (40)

Visualization

100 Per Page

Format

Preview

| resource | useragent | count |
|------------------|--|-------|
| /cart.do | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 788 |
| /cart.do | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 696 |
| /cart.do | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 572 |
| /product.screen | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 594 |
| /product.screen | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 488 |
| /cart.do | Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) | 432 |
| /oldlink | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 428 |
| /product.screen | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 408 |
| /product.screen | Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) | 368 |
| /category.screen | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 364 |
| /oldlink | Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) | 344 |
| /oldlink | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 324 |
| /category.screen | Googlebot/2.1 (http://www.googlebot.com/bot.html) | 316 |

