DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON TWO

Agenda

- Splunk Search
- Field Extraction
- Field Extraction with Regular Expressions
- Statistics

Splunk Commands

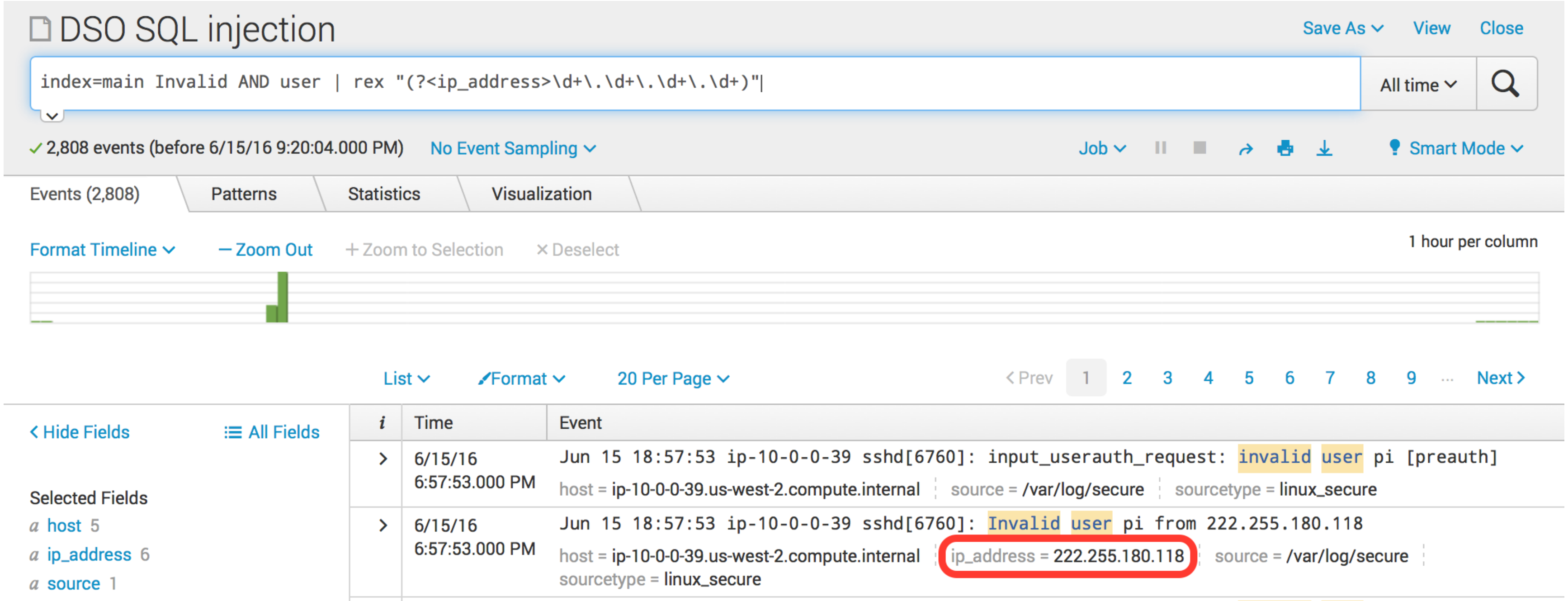
- Splunk Search
  - Retrieves events from indexes
  - Filters results of a previous search
  - Uses Search Processing Language
  - Implicit command when a search is performed or can be used further filter search results, e.g., `index=main sourcetype=linux_secure | search field=value`

Splunk Commands

- Field Extraction
  - Key value pairs extracted by Splunk or by custom field extraction
  - Used by splunk to
  - Commands used to perform field extraction: rex, rename, stats, etc.

Splunk Commands

- Field Extraction with Regular Expressions
  - rex – uses Perl like regular expression to extract fields from search results



```
index=main Invalid AND user | rex "(?<ip_address>\d+\.\d+\.\d+\.\d+)"
```

✓ 2,808 events (before 6/15/16 9:20:04.000 PM) No Event Sampling

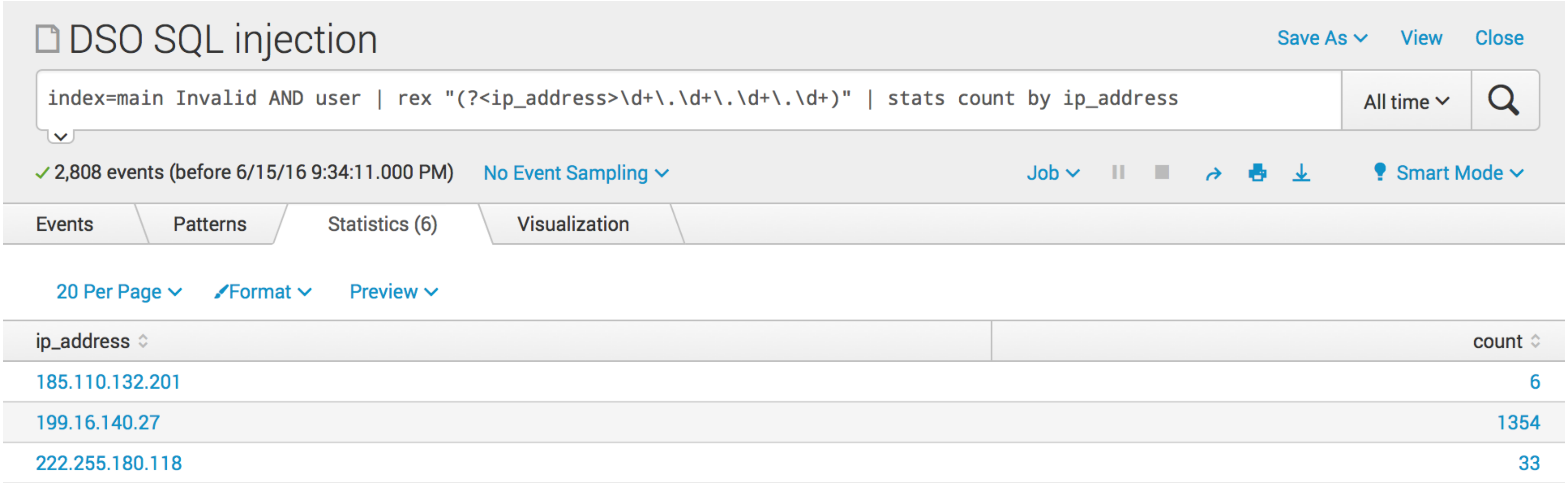
Selected Fields

- a host 5
- a ip_address 6
- a source 1

i	Time	Event
>	6/15/16 6:57:53.000 PM	Jun 15 18:57:53 ip-10-0-0-39 sshd[6760]: input_userauth_request: invalid user pi [preauth] host = ip-10-0-0-39.us-west-2.compute.internal · source = /var/log/secure · sourcetype = linux_secure
>	6/15/16 6:57:53.000 PM	Jun 15 18:57:53 ip-10-0-0-39 sshd[6760]: Invalid user pi from 222.255.180.118 host = ip-10-0-0-39.us-west-2.compute.internal · ip_address = 222.255.180.118 · source = /var/log/secure · sourcetype = linux_secure

Splunk Commands

- Statistics
  - `stats` command - calculates statistics such as counts, averages, min and max values



DSO SQL injection

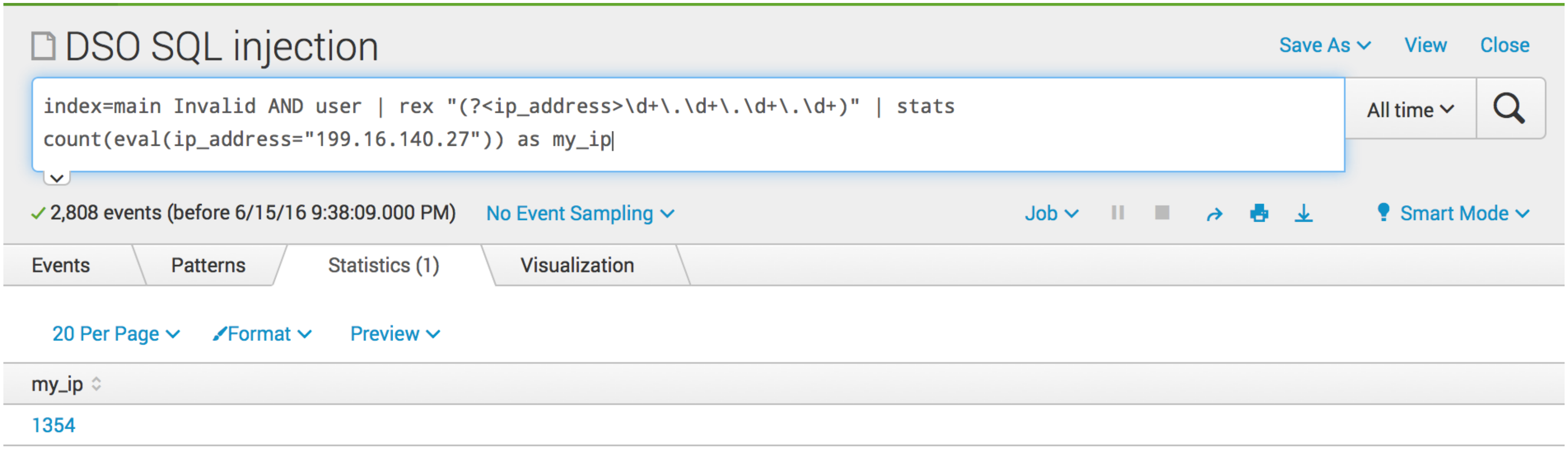
```
index=main Invalid AND user | rex "(?<ip_address>\d+\.\d+\.\d+\.\d+)" | stats count by ip_address
```

✓ 2,808 events (before 6/15/16 9:34:11.000 PM)

ip_address	count
185.110.132.201	6
199.16.140.27	1354
222.255.180.118	33

Splunk Commands

- Evaluating Fields
  - To narow in on a specific IP address for example, we could use a combination of count and eval to perform our query



DSO SQL injection

```
index=main Invalid AND user | rex "(?<ip_address>\d+\.\d+\.\d+\.\d+)" | stats
count(eval(ip_address="199.16.140.27")) as my_ip
```

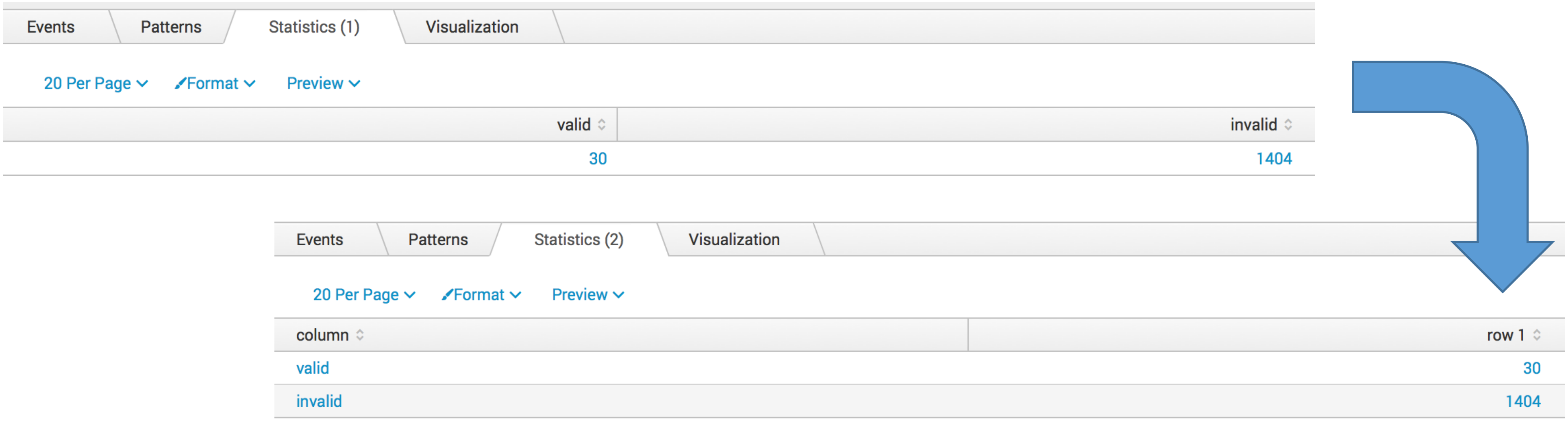
All time

✓ 2,808 events (before 6/15/16 9:38:09.000 PM)

my_ip
1354

Splunk Commands

- Tables and Visualization
  - transpose – converts rows into columns
    - helps us create charts souch as pie charts



valid	invalid
30	1404

column	row 1
valid	30
invalid	1404

Questions?

Lab 2

- If you weren’t here last week team up with someone who was or quickly do week 3 lab 2 (get AWS credentials from Instructor)

- If you were here last week:
  - Run through the exercises in week 3 lab 3 if Splunk searches return no data