

---

# DEV/SECOPS 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`

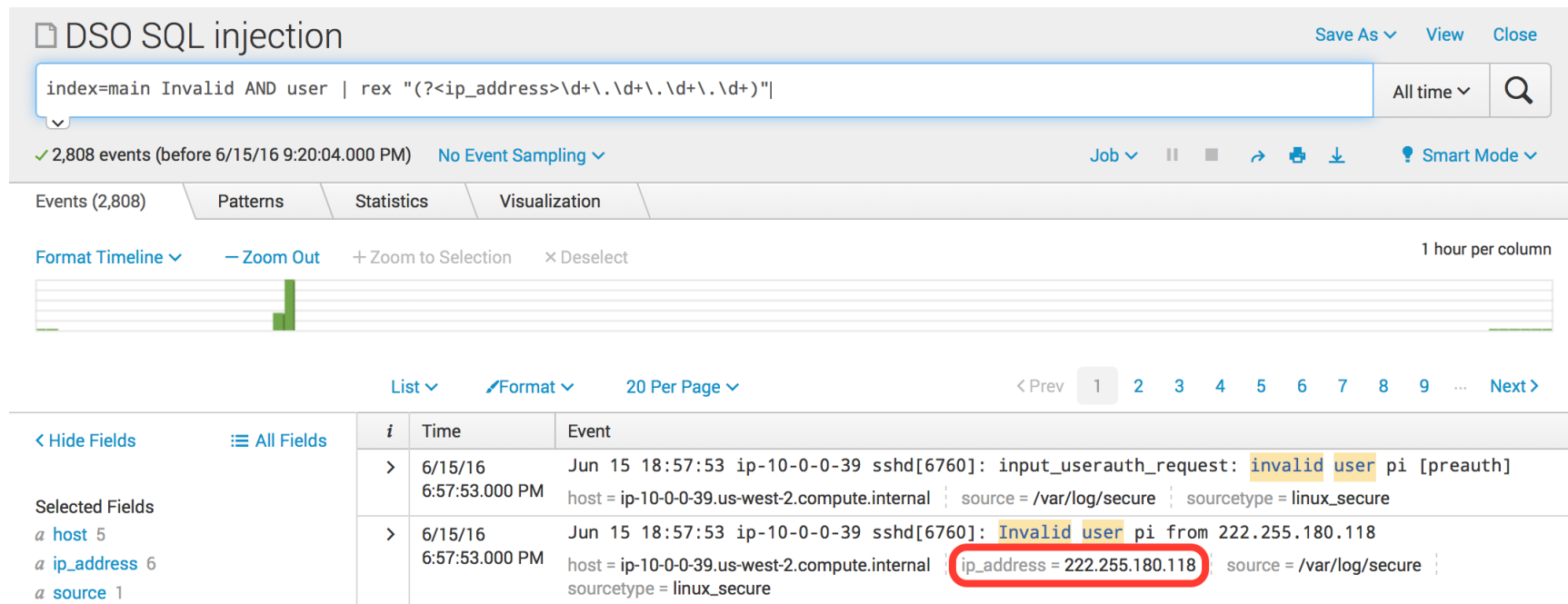
---

# 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



DSO SQL injection

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

Events (2,808) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields

Selected Fields

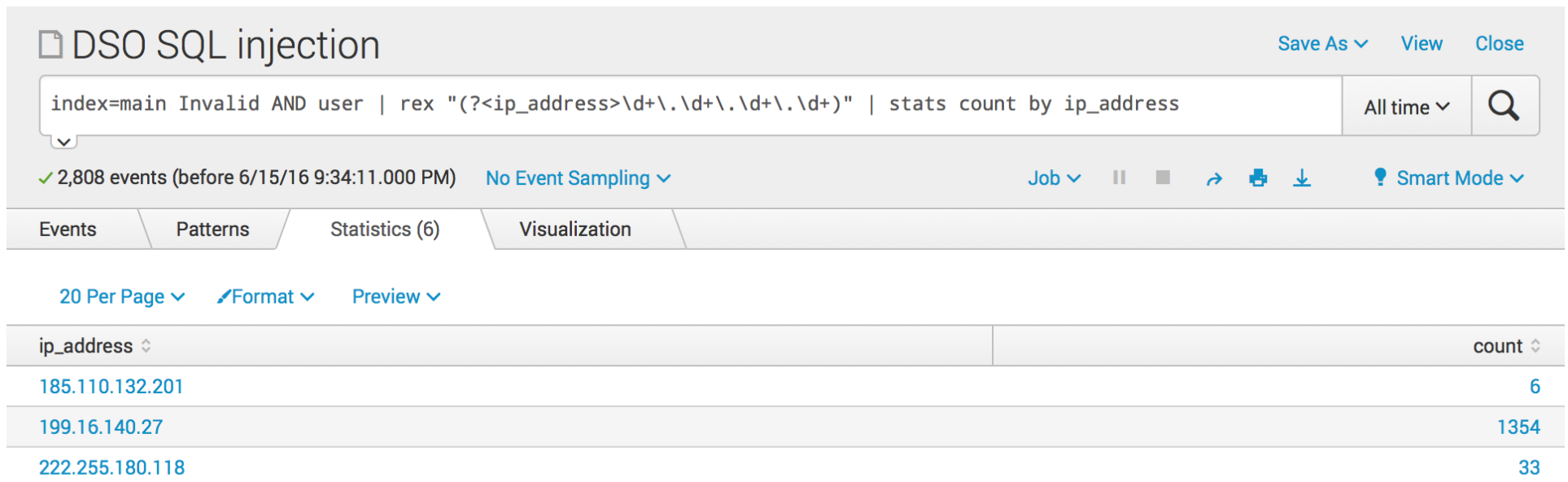
- host 5
- ip\_address 6
- source 1

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



The screenshot shows the Splunk search interface. The search bar contains the query: `index=main Invalid AND user | rex "(?<ip_address>\d+\.\d+\.\d+\.\d+)" | stats count by ip_address`. The results are displayed in a table with two columns: `ip_address` and `count`. The table shows three entries: `185.110.132.201` with a count of 6, `199.16.140.27` with a count of 1354, and `222.255.180.118` with a count of 33. The interface also shows a status bar indicating 2,808 events and various controls like 'Save As', 'View', 'Close', 'All time', and 'Smart Mode'.

ip_address	count
185.110.132.201	6
199.16.140.27	1354
222.255.180.118	33

# Splunk Commands

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

The screenshot shows the Splunk search interface. At the top, the search bar contains the query: `index=main Invalid AND user | rex "(?<ip_address>\d+\.\d+\.\d+\.\d+)" | stats count(eval(ip_address="199.16.140.27")) as my_ip|`. Below the search bar, the results are displayed in a table with the following columns: Events, Patterns, Statistics (1), and Visualization. The 'Statistics (1)' column shows a single row with the value '1354' under the field 'my\_ip'. The interface also includes a 'Save As' dropdown, 'View' and 'Close' buttons, a search icon, and a 'Smart Mode' toggle.

DSO SQL injection

Save As View Close

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) No Event Sampling

Job

Events Patterns Statistics (1) Visualization


20 Per Page Format Preview

my\_ip

1354

# Splunk Commands

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



Events	Patterns	Statistics (1)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	
		valid ▾	invalid ▾
		30	1404

Events	Patterns	Statistics (2)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	
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