
DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON TWO

Agenda

- Field Extraction
- Field Extraction with Regular Expressions
- Statistics
- Dashboards
- Alerts

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 displays 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|`. The results bar shows "2,808 events (before 6/15/16 9:38:09.000 PM)" and "No Event Sampling". The interface includes tabs for "Events", "Patterns", "Statistics (1)", and "Visualization". Below the tabs, there are options for "20 Per Page", "Format", and "Preview". The "Statistics (1)" tab is active, showing a single field named "my_ip" with a value of "1354".

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

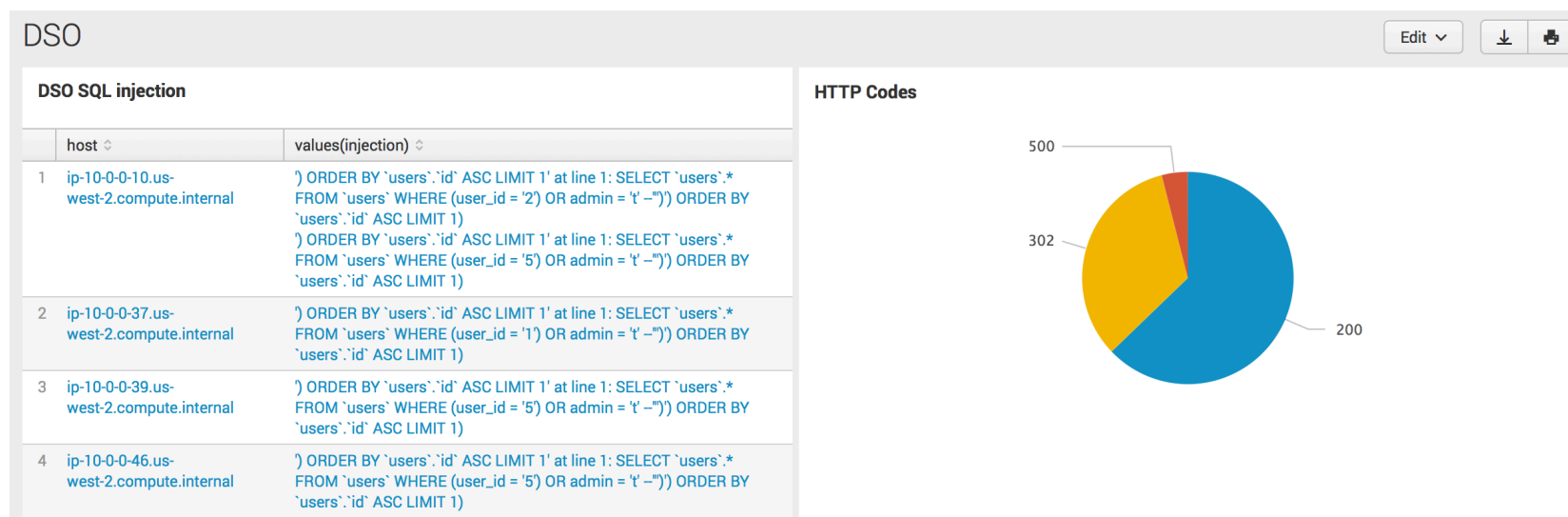


Events	Patterns	Statistics (1)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	
		valid ▾	invalid ▾
		30	1404

Events	Patterns	Statistics (2)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	
column ▾		row 1 ▾	
valid		30	
invalid		1404	

Dashboards

- Reveals trends
- Show security relevant or interesting events
- Real time high-level view of environment



Alerts

- Alerts can be used to
 - Drive a report
 - Send an email
 - Execute a Splunk app
 - Execute a custom script
 - Initiate incident response

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