

## Splunk - Failed SSH logins

**Problem:** identify whether there are any possible security issues with the mail server.

**Goal:** Explore any failed SSH logins for the root account.

**Process:**

- Upload data into Splunk
- Navigate to Search and Reporting tab, enter index=main host=mailsv fail\* root
- Results:

The screenshot displays the Splunk Search interface. At the top, the navigation bar includes 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar. Below this, the 'Search' tab is selected, with other tabs like 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards' visible. The 'New Search' section shows the search query 'index=main host=mailsv fail\* root' and indicates '346 events (before 10/02/2024 12:46:46.000)'. The 'Events (346)' tab is active, showing a timeline view and a list of events. The list view shows three events, all with a status of 'Failed' and a user of 'root'. The events are from the mailsv host, sourced from tutorialdata.zip/mailsv/secure.log, and have a sourcetype of secure-2. The interface also includes a 'Format Timeline' button, a 'Zoom Out' button, and a 'List' button. The 'Selected Fields' section shows 'host', 'source', and 'sourcetype'. The 'Interesting Fields' section shows 'date\_hour' and 'date\_minute'.

i	Time	Event
>	06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv! sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv   source = tutorialdata.zip/mailsv/secure.log   sourcetype = secure-2
>	06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv! sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2 host = mailsv   source = tutorialdata.zip/mailsv/secure.log   sourcetype = secure-2
>	06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv! sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2 host = mailsv   source = tutorialdata.zip/mailsv/secure.log   sourcetype = secure-2