

As part of my investigation into failed SSH login attempts for the root account on the mail server, I narrowed the search results by using the code `index=main host=mailsv` in Splunk. This allowed me to focus on relevant data related to unsuccessful login attempts. By honing in on this information, I can effectively analyze potential security issues associated with the root account.

The screenshot shows the Splunk Cloud interface with a search bar containing `index=main host=mailsv`. The search results show 9,829 events. The interface includes a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS', a main table of results, and a timeline visualization at the top.

Time	Event
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0) host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2

I used the code `index=main host=mailsv fail*` to narrow the search results to events generated by the mail server. Next, I continued to refine the search to specifically locate any failed SSH login attempts for the root account. This focused approach allows me to effectively identify potential security issues related to unauthorized access attempts.

The screenshot shows the Splunk Cloud interface with a search bar containing `index=main host=mailsv fail* root`. The search results show 346 events. The interface includes a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS', a main table of results, and a timeline visualization at the top.

Time	Event
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[3912]: Failed password for root from 109.169.32.135 port 4253 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5838]: Failed password for root from 223.205.219.67 port 3230 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1151]: Failed password for root from 175.44.1.122 port 1202 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[3789]: Failed password for root from 121.9.245.177 port 2691 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1799]: Failed password for root from 94.229.0.21 port 3983 ssh2 host = mailsv source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2