

# Splunk File Analysis

## Scenario:

I am a security analyst working at a fictitious e-commerce store. I have been tasked with identifying whether there are any possible security issues with the mail server. To do so, I must explore any failed SSH logins for the root account.

## Narrow search to the mail server

Because I have been tasked with exploring any failed SSH logins for the root account on the mail server, I will need to narrow the search results for events from the mail server. I accomplished this by locating the **SELECTED FIELDS** tab, selecting **host**, and then selecting **mailsv** to narrow my search to the appropriate area.

The screenshot displays the Splunk Cloud interface with a search bar containing the query `index="main" host="mailsv"`. The search results show 9,829 events. The **SELECTED FIELDS** tab is active, showing a list of fields including `host`, `source`, and `sourcetype`. The `host` field is selected, and the results are filtered to show only events from the `mailsv` host. The results table shows several failed SSH login attempts for the `root` user from various IP addresses. The interface includes a sidebar with navigation options, a top navigation bar, and a search bar.

Time	Host	Source	Sourcetype	Event
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Invalid user appserver from 194.8.74.23 port 3351 ssh2
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Invalid user testuser from 194.8.74.23 port 3626 ssh2
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Invalid user mongod from 194.8.74.23 port 2472 ssh2
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Invalid user mail from 194.8.74.23 port 1552 ssh2
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Invalid user games from 194.8.74.23 port 3887 ssh2
3/6/23 1:39:51:000 AM	mailsv	tutorialdata.zip/mailsv/secure.log	secure-2	Server listening on :: port 22.

## Search for a failed login for root

After successfully narrowing the search results to events generated by the mail server, I continued to narrow the search to locate any failed SSH logins for the root account. I accomplished this by entering `index="main" host="mailsv" fail* root` into the search bar. This search expands on the search from the previous task and searches for the keyword `fail*`. The wildcard i.e., asterisk symbol, tells Splunk to expand the search term to find other terms that contain the word fail such as failure, failed, etc. Lastly, the keyword `root` searches for any event that contains the term root.

**splunkcloud** Apps Messages Settings Activity Find

Search Analytics Datasets Reports Alerts Dashboards

**Search & Reporting**

**New Search** Save As Create Table View Close

index=main host=mailsv fail= root

✓ 346 events (before 9/30/24 10:34:22.000 PM) No Event Sampling

Job Policy-Based Pool Smart Mode

Events (346) Patterns Statistics Visualization

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

List Format 20 Per Page

Time	Event
3/6/23 1:39:51:000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1099]: 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 3238 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[11513]: Failed password for root from 175.44.1.122 port 1282 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	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1799]: Failed password for root from 94.229.8.21 port 3983 ssh2

SELECTED FIELDS: host 1 source 1 sourcetype 1

INTERESTING FIELDS: date\_hour 1 date\_mday 8 date\_minute 1 date\_month 2 date\_second 1 date\_wday 7 date\_year 1 date\_zone 1 index 1 linecount 1 punct 1 splunk\_server 1 timeendpos 1 timestamp 1

+ Extract New Fields

## Conclusion

Using Splunk, I have identified all relevant instances of failed SSH logins for the root account. Since there have been hundreds of failed SSH logins for the root account, investigating these events further will require obtaining a whitelist of IP addresses, and then cross-referencing that list with the results. Additionally, the time the login attempts occurred will also be worth noting to check for off-hours login attempts even from approved devices.