

Scenario

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

Directions:

1. If you haven't already, download the data file from Step 1: [tutorialdata.zip](#). Click the link then click the download icon. Do not uncompress the file.
2. Navigate to Splunk Home from your Splunk Cloud free trial instance. You might need to log in again using your credentials from Step 3.
3. On the Splunk bar, click Settings. Then click the Add Data icon.
4. Click Upload.
5. Click the Select File button.
6. Upload the **tutorialdata.zip** file, and click Open.
7. Click the Next button to continue to Input Settings.
8. By the Host section, select Segment in path and enter 1 as the segment number.

Click the Review button and review the details of the upload before you submit. The details should be as follows:

Input Type: Uploaded File

File Name: tutorialdata.zip

Source Type: Automatic

Host: Source path segment number: 1

9. Index: Default
10. Click Submit. Once Splunk has ingested the data, you will receive confirmation that the file was successfully uploaded.

The screenshot shows the Splunk Cloud interface with a search for `index=main`. The search results show 109,864 events. The interface includes a search bar, navigation tabs (Search, Analytics, Datasets, Reports, Alerts, Dashboards), and a list of event details. The event details table shows columns for Time and Event, with rows for events from 3/6/23.

Time	Event
3/6/23 6:24:02.000 PM	[06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = vendor_sales source = dataforsplunk.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:46.000 PM	[06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = vendor_sales source = dataforsplunk.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:31.000 PM	[06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = vendor_sales source = dataforsplunk.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:59.000 PM	[06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = vendor_sales source = dataforsplunk.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:48.000 PM	[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = vendor_sales source = dataforsplunk.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales

*Over 100,000 events in the main index!

Because you've been tasked with exploring any failed SSH logins for the root account on the mail server, you'll need to narrow the search results for events from the mail server.

Under SELECTED FIELDS, click host and click mailsv.

Notice that a new term has been added to the search bar: `index=main host=mailsv`.

The search results have narrowed to over 9000 events that are generated by the mail server.

The screenshot shows the Splunk Cloud interface with a search for `index=main host=mailsv fail* root`. The search results show 346 events. The interface includes a search bar, navigation tabs (Search, Analytics, Datasets, Reports, Alerts, Dashboards), and a list of event details. The event details table shows columns for Time and Event, with rows for events from 3/6/23.

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 = dataforsplunk.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 = dataforsplunk.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 = dataforsplunk.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 = dataforsplunk.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 = dataforsplunk.zip./mailsv/secure.log sourcetype = secure-2

Key takeaways

In this activity, we used Splunk Cloud to perform a search and investigation. Using Splunk Cloud, we were able to:

- Upload sample log data
- Search through indexed data
- Evaluate search results
- Identify different data sources
- Locate failed SSH login(s) for the root account