**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:**  02/25/24 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | I've been tasked with identifying whether there are any possible security issues with the mail server. I was tasked with creating a splunk account, uploading mock data into Splunk, performing basic searches, evaluating fields, searching for failed logins for root, and evaluating my search results | | |
| Tool(s) used | Splunk | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? n/a * **What** happened? n/a * **When** did the incident occur? n/a * **Where** did the incident happen? n/a * **Why** did the incident happen? n/a | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |