**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:** Mar 4, 2024 | **Entry:** #2 |
| Description | Suspicious Hash Notes |
| Tool(s) used | VirusTotal |
| The 5 W's | * **Who**: Unethical hacker(s) * **What**: Phishing attack * **Where**: Financial services company * **When**: Monday morning 1:11 PM * **Why**: The hackers launched the attack using phishing mails. Downloading the phishing email’s attachment triggered a download of unauthorized executables. |
| Additional notes | 1. The IDS alerted the SOC team on detection of executables 2. The SHA256 hash of the file was searched on VirusTotal 3. The file was found to be malicious and flagged accordingly |