**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:** June 08, 2024 | **Entry:** #3 |
| Description | Documenting a phishing incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: Clyde West * **What**: A Resume & Cover Letter (bfsvc.exe) ran arbitrary scripts * **Where**: At a Financial Services company, mx server * **When**: July 20, 2022 09:30:14 AM * **Why**: The incident happened is that the company's systems were sent phishing mail. So, employee opened the attachment, that ran arbitrary scripts. |
| Additional notes | 1. How could the finance services company prevent an incident like this from occurring again? 2. Can the hash of the file, help us understand its origins & purpose? |