**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 07, 2024 | **Entry:** #2 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: N/A * **What**: A Trojan / Backdoor incident * **Where**: At a Financial Services company * **When**: 1:20 PM * **Why**: The incident happened because the company's systems were accessed using a phishing attack. |
| 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? |