**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:** Feb 29, 2024 | **Entry:** #1 |
| Description | Ransomware Attack Notes |
| Tool(s) used | Nil |
| The 5 W's | * **Who**: Organized group of unethical hackers * **What**: Ransomware attack * **Where**: Health care clinic * **When**: Tuesday morning 9:00 AM * **Why**: The hackers used phishing mails to gain access to the company network. Clicking on the phishing email’s attachment downloaded malware. Using this ransomware, the hackers encrypted the critical files of patients. The ransom demands a large sum of money to decrypt the files back. |
| Additional notes | 1. The clinic should invest in IDS and anti-malware software 2. The clinic should conduct quarterly cybersecurity training |