**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:**  August 19, 2025 | **Entry:**  #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An organized group of unethical hackers. * **What** happened? A ransomware security incident. * **When** did the incident occur? Tuesday at 9:00 a.m. * **Where** did the incident happen? At a healthcare company. * **Why** did the incident happen? A phishing attack was successful via the computer’s systems on the healthcare network. Promptly after gaining access, the hackers installed ransomware to encrypt any relevant critical files. The motive associated with such an attack is most likely financial based as they requested a large sum of money for payment in exchange for the decryption key. |
| Additional notes | The healthcare company should heavily consider utilizing backups for mitigation purposes in the future as this would help bypass the necessity for paying ransomware in the future.  If there is no other option, then the company will likely have to gamble and pay for the decryption key due to critical files being necessary for patient’s cases. |

|  |  |
| --- | --- |
| **Date:**  August 19, 2025 | **Entry:**  #2 |
| Description | Analyzing a packet capture file |
| Tool(s) used | Wireshark – a network protocol analyzer |
| 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 | Wireshark is generally new to me, so there was much to catch up regarding the analysis of packet captures. There is a lot going on in this environment, so it is understandable that there are specialists with software such as network protocol analyzers. |

|  |  |
| --- | --- |
| **Date:**  August 19, 2025 | **Entry:**  #3 |
| Description | Capturing my first packet |
| Tool(s) used | Tcpdump – capture and analyze network traffic |
| 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 | Utilizing the command-line interface is still relatively new to me, so the entire process is challenging. Understanding the various commands seems to be the biggest choke point for me at the moment. Repetition in a real environment would help a lot. |

|  |  |
| --- | --- |
| **Date:**  August 19, 2025 | **Entry:**  #4 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | VirusTotal – investigative tool that analyzes files and URLs for malicious content. It is incredibly helpful for checking IoCs for legitimacy.  This incident occurred in the Detection and Analysis phase and had me in the perspective of a junior SOC Analyst investigating the hash file. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An unknown malicious actor * **What** happened? An email sent to an employee contained a malicious file attachment with a SHA-256 file hash. * **When** did the incident occur? At 1:20 p.m., an alert was received by the organization’s SOC after the IDS detected the file. * **Where** did the incident happen? An employee’s computer in the financial services company. * **Why** did the incident happen? An employee was able to download and execute a malicious file attachment via email. |
| Additional notes | Future incidents regarding this issue would be better social engineering training for various departments. |

|  |
| --- |
| Reflections/Notes: I found various commands involving the process of using tcpdump rather challenging because there is a lot to unpack and understand when it comes to filtering data with in a CLI environment. The activity took me longer than I anticipated.  My total understanding and awareness for incident detection grew with this course because it highlighted such a large knowledge base that I knew very little about. The complexity levels definitely began to show through when going over each of the assignments.  I enjoyed the data capture and analysis tools because it makes me feel like I understand the beginning of what data on a network is and what it is doing, which is foundational for a career in Cybersecurity. |