**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:**  8.19.23 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Sample ransomware attack | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | * Group of unethical hackers known for conducting similar attacks on other healthcare and transportation companies attacked through employees * Hackers used phishing emails to deploy ransomware on the target computers, locking out critical patient data. They demand a large ransom. The company was forced to shut down their systems. * Occurred on Tuesday, ~9 am * Incident was reported when employees found ransom notes on their displays and were locked out of data. * Hacker group attempted such an attack to receive a large amount of money from the organization | | |
| Additional notes | Several organizations were contacted for technical assistance. | | |

| **Date:**  8.26.23 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Analyzing packets on wireshark | | |
| Tool(s) used | Wireshark | | |
| The 5 W's | * I was the one analyzing packets from a sample organization * Using Wireshark, I used filters to search for and analyze specific packets, extracting useful information from the logs. * The event was practice for using Wireshark, filtering out specific packets by protocol, ip, etc. | | |
| Additional notes | It’s useful to know many possible filters/filter types or where to find . | | |

| **Date:**  8.27.23 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Using tcpdump to capture packets, a command-line packet sniffer. I filtered, captured, and examined packets. | | |
| Tool(s) used | tcpdump | | |
| Additional notes | Some of the information shown was overwhelming or unintuitive. It helps to break down commands and output and comprehend each part separately. | | |

| **Date:**  8.27.23 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Suspicious hash research | | |
| Tool(s) used | VirusTotal, a community tool that checks if files, urls, hashes, etc are malware based on its behavior in a sandbox and the community’s experience with it. | | |
| The 5 W's | Capture the 5 W's of an incident.   * Threat actor * An email sent to an employee had malicious downloads embedded in it. They downloaded themselves onto the computer and were detected by IDS. Their SHA-256 hash was then investigated. * 1;20pm * Employee desktop * An employee downloaded and executed a file sent via email. | | |
| Additional notes | Next step would be preventing similar occurrences. Might consider educating employees or automatically block files that aren’t of a specific type. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |