**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:** 28-Dec-2023 | **Entry:** #1 | | |
| --- | --- | --- | --- |
| Description | Document of a cybersecurity incident | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers * **What**: A ransomware * **When**: Tuesday at 9:00 a.m. * **Where**: A small U.S. health care clinic * **Why**: The group of hackers sent a phishing email to one of the employees, containing a malicious attachment. Once downloaded, the ransomware that the group had designed before, was executed on its own and encrypted the data on the server. The attackers demanded money to decrypt the files, showing financial reasons as their motivation. | | |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? | | |

| **Date:**  2-Jan-2024 | **Entry:** #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | * Wireshark | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | This was my first time using Wireshark, and I was thrilled to start this exercise and examine a packet capture file. At the outset, the interface seemed quite daunting, but I can comprehend why it is such a potent tool for comprehending network traffic. | | |

| **Date:**  2-Jan-2024 | **Entry:** #3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | * tcpdump | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A | | |
| Additional notes | Even though this was my initial exposure to tcpdump, I'm quite acquainted with the command-line interface. Therefore, capturing and filtering network traffic using tcpdump was a delightful experience for me. | | |

| **Date:**  2-Jan-2024 | **Entry:** #4 |
| --- | --- |
| Description | Document of a cybersecurity incident |
| Tool(s) used | * SHA256 hash * VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unknown email sender * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When**: The intrusion detection system detected the file at 13:20 and sent an alert to the organization's SOC. * **Where**: On a single employee’s device at a financial service company * **Why**: A malicious file attachment was downloaded and executed via email by one of the employees. |
| Additional notes | In what ways can we prevent such incidents from happening again? Is it worth considering enhancing security awareness training to ensure employees are cautious about clicking on suspicious links? |

| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   Although this can not be counted as challenging, I had problems signing up in Splunk and Chronicle, due to my nationality and where I live, currently. Therefore, I couldn’t find a way to experience these tools to get myself familiar to them. However, if there is a chance to get familiar with them to make my path in cybersecurity more knowledgeable, I would definitely capture the opportunity to use and master these tools.   1. **Has your understanding of incident detection and response changed after taking this course?**   Even though I have never worked in cybersecurity, due to my background in computer science and blockchain, I had a pretty good insight about security incidents and events. However, taking this course introduced many useful tools to me, which I will be delighted to use. |
| --- |