**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:** Dec, 17 2024 | **Entry: #1** | | |
| --- | --- | --- | --- |
| Description | A Cybersecurity Incident. | | |
| Tool(s) used | **Nothing.** | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers * **What**: Ransomware of systems * **When**: Tuesday 9:00 am. * **Where**: At a health care company. * **Why**: Using a targeted phishing emails the attackers gained access to the system and installed ransomware that encrypts all data, they seems to do that for the financial gains given the note they kept to sell the decryption key for getting the data back. | | |
| Additional notes | 1. What can the company do to retrieve the data? 2. How did the employees fall for a simple phishing email? | | |

| **Date:**  Dec 31, 2024 | **Entry: #2** | | |
| --- | --- | --- | --- |
| Description | Analyzing packets with Wireshark | | |
| Tool(s) used | I used Wireshark to analyze a packet capture file or a ‘pcap’ file, and with using wireshark queries to search through the logs I was able to capture and detect some malicious activities in the network traffic captured. | | |
| 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 | I used Wireshark before, but after this course I learned some new queries and that was helpful in finding interesting data in a packet capture. | | |

| **Date:**  Dec 31, 2024 | **Entry: #3** | | |
| --- | --- | --- | --- |
| Description | Using TCPdump to capture network traffic | | |
| Tool(s) used | Tcpdump is the CLI Command-line interface network analyzer that works similar to wireshark with different syntax but it is lightweight and you can find it in any unix system which makes analyzing traffic easier whatever machine you use. | | |
| 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 | I find it more fun using the CLI since I can use other tools with the tcpdump output like grep and others, which makes it fun to work with and it gives me more power. | | |

| **Date:**  Jun 1, 2025 | **Entry: #4** | | |
| --- | --- | --- | --- |
| Description | Investigate a malicious file hash | | |
| Tool(s) used | We used VirusTotal to analyze the file for malicious content like viruses, it is a nice tool to quickly check for any URL or file before using and in this task we did just that but instead of a file we had the hash of the file which can be checked the same way. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Malicious actor. * **What:** An email was sent to one of the HR team containing a .exe file attachment. * **When**: At 1:20 pm * **Where**: financial services company. * **Why**: the employee downloaded the exe file and it was executed. | | |
| Additional notes | Should we give employees more knowledge about how to deal with any attachment file or URL? | | |

| **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. | | |

| **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. | | |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

| Reflections/Notes:  I found most of the activities in the course to be quite easy, especially analyzing packets with Wireshark since I had some experience with it before. Learning new queries made it even simpler to find important information in the data. My understanding of incident detection and response has definitely improved, especially in how different tools can help analyze network traffic. I really enjoyed using TCPdump because it is lightweight and fun to work with in the command line. This hands-on experience has shown me how important practical skills are in cybersecurity. Overall, the course has given me helpful insights and techniques that I look forward to using in the future. |
| --- |