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: 10/08/2023	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	● **Who** : An organized group of unethical hackers ● **What** : A ransomware attack incident ● **When** : Tuesday 9:00 a.m. ● **Where** : A healthcare company ● **Why** : The motive is financial because the attackers demanded huge amount of money in exchange for the decryption key so that the system will run back to normal.
Additional notes	1. How to prevent incidents like this happening again in future? 2. Does the healthcare company pay the attackers to get the decryption key?

Date: Record the date of the journal entry.	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	Wireshark. Wireshark is a packet sniffer.
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 is the first time I am using Wireshark. I am so happy to gain a packet capturing and analyzing skill using this tool. At beginning, it was a bit overwhelming but it gets comfortable overtime.

Date: Record the date of the journal entry.	**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	Using the command-line interface to capture and filter network traffic was difficult for me because I'm still learning how to use it. I used the incorrect commands a few times, which caused me to get stuck. However, after carefully observing the guidelines and I was able to complete this exercise and acquire network traffic data by redoing a few stages.

Date: Record the date of the journal entry.	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	I utilised VirusTotal for this exercise, which is a research tool that scans files and URLs for harmful stuff like viruses, worms, trojan horses, and more. If you want to rapidly determine whether a website or file that may be a sign of compromise has been flagged as malicious by other members of the cybersecurity community, utilise this tool. In order to complete this task, I used VirusTotal to examine a file hash that had been flagged as dangerous. During the Detection and Analysis phase, an occurrence happened. I was put in the position of a security analyst at a SOC looking into a suspicious file hash

	in the scenario. I had to conduct more thorough research and analysis after the security measures in place identified the suspicious file to ascertain whether the alert indicated a legitimate threat.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** Unknown malicious actor ● **What: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b** ● **Where: An employee's computer at a financial services company** ● **When: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file** ● **Why: An employee was able to download and execute a malicious file attachment via e-mail.**
Additional notes	How may this occurrence be avoided in the future? Should we think about enhancing security awareness training so that staff members are cautious about the links they click on?

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: Record additional notes.
1. Were there any specific activities that were challenging for you? Why or why not? The tcpdump activity was quite difficult for me. Learning the syntax for a tool like tcpdump was a significant learning curve for me because I am new to utilizing the command line. I initially experienced a lot of frustration because I wasn't obtaining the desired results. I redone the exercise to identify my mistakes. I took away from this experience the need to carefully follow the directions and go gently. 2. Has your understanding of incident detection and response changed after taking this course? My understanding of incident detection and response has clearly changed as a result of attending this course. I had a basic understanding of detection and reaction at the start of the course, but I wasn't entirely aware of how intricate it was. As I moved through the training, I discovered the incident lifecycle, the value of strategies, processes, and people, as well as the tools employed. Overall, I believe that my understanding of incident detection and response has evolved, and I am now better informed and equipped. 3. Was there a specific tool or concept that you enjoyed the most? Why? I really enjoyed learning about network traffic analysis and using network protocol analyzer tools to put what I had learned to use. It was tough and thrilling for me to learn about network traffic analysis for the first time. The ability to employ technologies to record network traffic and analyze it in real time greatly intrigued me. I have a greater desire to study more about this subject and eventually improve my ability to use network protocol analyzer tools.