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: 9.3.2025	**Entry: #**1
Description	Documenting a cybersecurity incident. This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance.
Tool(s) used	None.
The 5 W's	● **Who** caused the incident? An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. ● **What** happened? A ransomware security incident. ● **When** did the incident occur? On Tuesday at 9 am. ● **Where** did the incident happen?

	At a small U.S. health care clinic. ● **Why** did the incident happen? The incident happened because phishing email was sent to several employees of the company, which contained a malicious attachment. Once it was downloaded, the attackers managed to get access to the organization's computer files, and encrypting them will demanding for a ransom. This is a type of ransomware and their motivation is financial gain, because they demanded a large sum of money in exchange for decryption key.
Additional notes	• How can the organization prevent security incident like this from happening again in the future? • Should the organization pay the ransom in exchange for the data, or is there any better solution?

Date: 10.3.2025	**Entry: #2**
Description	Documenting a cybersecurity incident involving data theft through ransomware.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An unknown malicious actor ● **What** happened? A data theft and ransomware security incident. ● **When** did the incident occur? December 28, 2022, at 7:20 p.m.

	● **Where** did the incident happen? At a mid-sized retail company ● **Why** did the incident happen? Based on the investigation, there is a vulnerability in the e-commerce web application. This vulnerability allowed the hacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the hacker to access customer purchase confirmation pages, exposing customer data, which the hacker then collected and exfiltrated.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 11.3.2025	**Entry: #3**
Description	Documenting a cybersecurity incident through a phishing attempt.
Tool(s) used	I used VirusTotal to analyze the suspicious attachment from the email. By keying the hash value inside VirusTotal, it can help to analyze if the file is malicious and gives information about possible malware associated with the hash, community score, etc. This incident occurred in the **Detection and Analysis** phase. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Unknown malicious actor. ● **What** happened? A phishing attempt through malicious attachment. An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When** did the incident occur? At 1:11pm ● **Where** did the incident happen? At a financial services company. ● **Why** did the incident happen? The company received an alert about a suspicious file being downloaded on an employee's computer. Upon investigation, it was discovered that the employee received an email containing an attachment. Once the file was downloaded and opened, a malicious payload was then executed on their computer.
Additional notes	

Date: 12.3.2025	**Entry: #4**
Description	Documenting methods of capturing packets using tcpdump.
Tool(s) used	I used tcpdump, which is used to capture network traffic. It is a command-line 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	Include any additional thoughts, questions, or findings.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

I really enjoyed using tcpdump, although it can be quite challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. Although Wireshark seems visually easier to read, I find tcpdump is better to see the codes clearly if something was off and with a few lines of code, you could instruct the system on what to do. What I learned from this was to carefully read the instructions and work through the process slowly. I also need to remember the commands and it does to be better at using tcpdump.

2. **Has your understanding of incident detection and response changed after taking this course?**

This course has significantly deepened my understanding of incident detection and response. Initially, I had a basic grasp of these concepts but didn't fully appreciate their complexity. As I advanced through the material, I gained insight into the incident lifecycle, the critical role of structured plans and processes, and the tools used for effective response. Overall, my perspective has evolved, and I now feel more knowledgeable and well-equipped to handle incident detection and response effectively.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. I found it really interesting to be able to use tools to capture network traffic and analyze it in real time. I am definitely more interested in learning more about this topic, and I hope to one day become more proficient in using network protocol analyzer tools.