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: **09-16-2025**	**Entry: 01**
Description	**Investigating a ransomware attack deployed through targeted phishing emails.**
Tool(s) used	**N/A**
The 5 W's	**Capture the 5 W's of an incident.** • **Who caused the incident? An organized, unethical hackers group.** • **What happened? Some employees reported being unable to access their computers. Notes were displayed on the computers stating that the organization needs to pay a substantial amount of money to decrypt their files.** • **When did the incident occur? It happened on a Tuesday at 9:00 a.m.** • **Where did the incident happen? The incident happened in a healthcare clinic.**

	• **Why did the incident happen? The incident happened because some employees downloaded malicious attachments from unsuspected targeted phishing emails. The downloaded attachments gave unethical hackers unauthorized access to the system, allowing them to deploy their ransomware successfully.**
Additional notes	**The company employees lacked awareness about phishing emails. The security controls on unauthorized downloads, lack of file scanning before and after downloads, and blocking of unauthorized application file access, unfortunately, led to the successful ransomware attack.**

Date: **09-18-2025**	**Entry: 02**
Description	**Analyzing a packet using tcpdump**
Tool(s) used	**Qwiklab, tcpdump (for network packets capture and analysis)**
The 5 W's	**Capture the 5 W's of an incident.** • **Who caused the incident? N/A** • **What happened? I used tcpdump to capture network data for inspection.** • **When did the incident occur? N/A, same as date** • **Where did the incident happen? At home** • **Why did the incident happen? The event happened because I wanted to gain practical experience of analyzing a network packet.**
Additional notes	**The activity is a great way of introducing the scope and capabilities of tcpdump.**

Date: **09-19-2025**	**Entry: 03**
Description	**Verifying and further investigating if an employee downloaded a malicious password-protected attachment from an email.**
Tool(s) used	**Virustotal, phishing playbook (file analysis)**
The 5 W's	**Capture the 5 W's of an incident.** • **Who caused the incident? The employee and the virus sender.** • **What happened? An employee accessed a password-protected email attachment that executed a malicious file. The malicious file's hash was investigated using Virustotal.** • **When did the incident occur? N/A** • **Where did the incident happen? In the workplace.** • **Why did the incident happen? It happened because a naïve employee downloaded and opened a malicious file.**
Additional notes	**Investigations can be done thoroughly using IOC detection tools such as Virustotal.**

Date: **09-19-2025**	**Entry: 04**
Description	**Reviewing a final report.**
Tool(s) used	**N/A**

The 5 W's	**Capture the 5 W's of an incident.** • **Who caused the incident? The accident was caused by an employee receiving a ransomware email.** • **What happened? The employee initially ignored a ransomware email from an attacker. A few days later, the same attacker sent a receipt of the data they had, confirming the data breach. The cybersecurity team investigated, responded to, and implemented mitigations after the attack.** • **When did the incident occur? The initial email was on December 22, 2022, at 3:13 pm PT. The second email was sent on December 28, 2022. The team investigated the incident from December 28 to December 31, 2022.** • **Where did the incident happen? It happened on site.** • **Why did the incident happen? The incident occurred due to a vulnerability in the organization's web application. It allowed the attacker to access customer purchase confirmation pages, exposing data that the attacker had collected and exfiltrated.**
Additional notes	**The final report was deemed comprehensive, detailing what happened, how the company handled the incident, and what recommendations should be implemented.**

Reflections/Notes: All activities were smooth sailing, and I did not encounter any challenging tasks. I think this is because of my background in cybersecurity, wherein is my undergraduate specialization. However, these activities did expand my knowledge and deepen my understanding of incident detection and response. I am thankful that these activities provided me with an opportunity to apply the

theoretical concepts I have learned about such topics. Overall, I enjoyed capturing and analyzing network traffic the most. Seeing what goes on under the tip of the iceberg is always refreshing and motivating because you just know more.