Incident handler's journal

Date: 29-08-2025	**Entry:** 1
Description	Entry on Ransomware attack on US health care clinic
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • The incident was caused by an organized group of unethical hackers that target organizations in the healthcare and transportation industries. • The group was able to encrypt critical files and softwares that were needed by the employees to do their job and demanded payment before revealing the key. They were able to achieve this with a phishing email that contained a malicious attachment, The ransomware was deployed once it was downloaded. • The incident occurred on Tuesday at 9:00AM • The incident occurred in the health care clinic's system • The incident occurred because one of the employees of the clinic clicked the link in the phishing email and gave the ransomware access into the system. The motivation of the hackers was to exploit the company financially
Additional notes	When a ransomware infection is detected, the affected system should immediately be quarantined to prevent lateral spread across the network. Restoration should then be performed using a clean backup taken prior to the compromise, ensuring both files and applications are recovered to a safe state. Beyond technical remediation, employees must be continuously educated on how to identify and report suspicious emails, since phishing is a common entry

	point for ransomware. To further reduce risk, the organization should enforce multi-factor authentication (MFA), deploy advanced email filtering solutions, and regularly run phishing simulations to test and improve employee awareness. Endpoint protection tools, combined with routine patch management, can also help reduce exposure to malicious payloads delivered through email. Together, these preventive and corrective measures strengthen resilience against phishing-based ransomware attacks.

Date: 02/09/2025	**Entry:** 2
Description	Entry on phishing attack on financial service company
Tool(s) used	Virus Total
The 5 W's	Capture the 5 W's of an incident. • The incident was caused by a malicious actor with the sender name Def communications who is associated with the email address 76tguy6hh6tgftrt7tg.su • The group is trying to attack the financial company with a phishing attack orchestrated with the use of an email phishing link sent to an employee. • The incident occurred on the 20th of July 2022 at about 09:30:14 AM • The incident occurred in an employee's computer

	• The incident occurred because one of the employees of the clinic clicked the link in the phishing email thereby downloading the malware
Additional notes	To reduce risk of phishing attacks, the company should enforce multi-factor authentication (MFA), deploy advanced email filtering solutions, and regularly run phishing simulations to test and improve employee awareness. Endpoint protection tools, combined with routine patch management, can also help reduce exposure to malicious payloads delivered through email. Together, these preventive and corrective measures strengthen resilience against phishing-based ransomware attacks.

Date: 07/09/2025	**Entry:** 3
Description	Analyzing packet capture file
Tool(s) used	For this task, I examined a packet capture file using Wireshark, a network protocol analysis tool with a graphical interface. In cybersecurity, Wireshark is especially valuable because it enables analysts to capture and review network traffic in detail, which is useful for identifying and investigating potential malicious activity.
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	Since this was my first time using **Wireshark**, I was eager to dive into the exercise and work with a packet capture file. The interface initially felt a bit overwhelming, but it quickly became clear why the tool is considered so powerful for examining and understanding network traffic.

Date: 07/09/2025	**Entry:** 4
Description	Capturing my first packet
Tool(s) used	In this exercise, I worked with tcpdump to capture and review network traffic. Tcpdump is a command-line based protocol analyzer, and much like Wireshark, its strength in cybersecurity lies in enabling analysts to capture, filter, and examine network communications in detail.
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	As someone still learning the command-line interface, I found capturing and filtering network traffic a bit challenging at first. I ran into issues when I entered incorrect commands, but by carefully reviewing the instructions and repeating

	a few steps, I was eventually able to complete the activity and successfully capture the traffic.

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	**Entry:** Record the journal entry number.

the journal entry.	
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?:**

   I found the tcpdump activity particularly difficult since I'm still getting used to working with the command line. Learning the proper syntax for tcpdump was a steep adjustment, and at first I was frustrated because my commands weren't producing the expected results. After redoing the task and double-checking my steps, I realized my mistakes. This taught me the value of slowing down and carefully following instructions. Most issues i faced where that of syntax

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

   Yes, my perspective on incident detection and response has grown significantly. Before starting the course, I only had a basic idea of what those processes involved. As I went through the lessons, I learned about the different stages of an incident, why structured plans and teams are so important, and the role of different tools in the process. I now feel that I have a deeper and more practical understanding of how incident detection and response work.

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

   One tool I found especially interesting was **VirusTotal**, which I used to investigate a file hash. I was impressed by how much information the platform provides, from antivirus detections to file behavior and threat intelligence sources. At the same time, it was also a bit challenging because of the sheer volume of data returned. Learning how to navigate through the different sections and interpret the most relevant details made the experience both educational and practical for understanding how analysts use threat intelligence tools.