Incident Handler's Journal

Overview

As part of my cybersecurity training, I developed an Incident Handler's Journal to practice documenting and analyzing simulated incidents. This project demonstrates my ability to track incident response phases, use investigative tools, and reflect on lessons learned.

Key Activities

1. Documenting a Ransomware Incident

- Recorded incident details using the 5 W's framework.
- Identified detection, analysis, containment, and recovery phases.
- Assessed prevention strategies such as phishing awareness training and system hardening.

2. Network Traffic Analysis with Wireshark

- Captured and analyzed packet data using Wireshark.
- Interpreted protocols and potential anomalies in a packet capture file.
- Gained familiarity with packet structure and how malicious activity may appear in traffic.

3. Capturing Traffic with tcpdump

- Used `tcpdump` on the command line to capture and filter traffic.
- Practiced applying capture filters to isolate relevant packets.
- Overcame syntax errors by iterating commands and debugging.

4. Investigating a Suspicious File Hash with VirusTotal

- Investigated a suspicious hash flagged by an IDS alert.
- Used VirusTotal to analyze the file hash and determine whether it was malicious.
- Applied incident response thinking by evaluating user behavior and recommending awareness training.

Table 1

Date: September 9, 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**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Table 2

Date: September 10 2025	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in

	cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.

Table 3

Date: September 11 2025	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic.

Table 4

Date: September 12, 2025	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. 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	• **Who**: An 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 can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

Reflections & Lessons Learned

- Developed stronger documentation skills for incident tracking.
- Learned the importance of detection and response lifecycle (Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned).
- Built confidence using network analysis tools despite challenges with command-line syntax.
- Realized that security awareness training is as important as technical defenses in preventing incidents.