# 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:** July 23, 2024 | **Entry:**<br>#1 |
|---|---|
| Description | Documenting a cybersecurity incident<br><br>This incident occurred in the two phases:<br>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.<br>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<br>• **What**: A ransomware security incident<br>• **Where**: At a health care company<br>• **When**: Tuesday 9:00 a.m.<br>• **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?**<br>The healthcare company should revisit its employee cybersecurity training, especially around phishing awareness and implement stronger email filtering and multi factor authentication.<br>2. **Should the company pay the ransom to retrieve the decryption key?**<br>While paying the ransom may seem like a fast resolution, it is legally and ethically discouraged and doesn't guarantee full data restoration.<br>Engaging law enforcement and incident response professionals is a better course of action. |

---

| | |
|---|---|
| **Date:** July 25 2024 | **Entry:**<br>#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**: Unknown actor (possibly APT or opportunistic threat group)<br>• **What**: Malicious executable file (identified through SHA-256 hash)<br>• **Where**: Likely spread via phishing email or malicious website (based on threat profile)<br>• **When**: Recently detected (based on submission date to VT and Sandbox reports)<br>• **Why**: Likely to steal credentials, establish remote access, or encrypt data for ransom |
| Additional notes | This exercise taught me how to trace the footprint of a specific file using only its hash. I learned how to interpret sandbox data, read behavioral analysis |

| | |
|---|---|
| | reports, and spot signs of malicious activity like unusual process creation, registry edits, and external network connections. It gave me insight into how threat intelligence is shared and used to respond to incidents in the real world. |

---

| | |
|---|---|
| **Date:** July 25 2025 | **Entry:**<br>#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**: Me as the analyst-in-training<br>• **What**: Captured live network packets using tcpdump<br>• **Where**: On local test system<br>• **When**: July 25, 2025, during my hands-on lab<br>• **Why**: To practice using tcpdump for packet capture and filtering, and to get more comfortable with command-line tools used in incident response. |
| Additional notes | As someone new to the command line, this exercise was challenging but rewarding. I ran into errors using incorrect flags and syntax, but after re-reading the instructions and troubleshooting step by step, I was able to capture and filter live network traffic. This help me build more confidence in using terminal-based tools, especially in environments without a GUI. |

---

| | |
|---|---|
| **Date:** July 27 2024 | **Entry:**<br>#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.<br><br>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<br>• **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b<br>• **Where**: An employee's computer at a financial services company<br>• **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file<br>• **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?**<br><br>To help prevent this type of incident in the future, the organization should consider strengthening its security awareness training.<br><br>**Should we consider improving security awareness training so that employees are careful with what they click on?**<br><br>Employees need to be better equipped to recognize and avoid suspicious emails and file attachments. It may also be worth evaluating the email and filtering and attachment scanning policies currently in place. Should we also improve the alert escalation process to ensure faster response times from the SOC? |

| **Date:**<br>July 20, 2022 | **Entry:**<br>#5 |
|---|---|
| Description | Server-Mail Phishing attempt possible download of malware |
| Tool(s) used | File Hash |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>Clive West (suspected phishing sender posing as job applicant)<br>● **What** happened?<br>A phishing email was sent to an HR employee. The message appeared to be a job application and may have contained malicious links or attachments.<br>● **When** did the incident occur?<br>Wednesday, July 20, 2022 at 0930:14<br>● **Where** did the incident happen?<br>Employees workstation at Financial Services Company<br>● **Why** did the incident happen?<br>● HR employee assumed the email and attachment was from a legitimate employee hopeful. |
| Additional notes | This appears to be a socially engineered phishing attempt exploiting HR workflows. It's unclear whether the file was executed or if malware was successfully installed, follow-up investigation needed. Consider implementing stricter email filtering rules, attachment sandboxing, and more aggressive security awareness training for HR personnel, especially related to hiring scams. Was VirusTotal or Sandbox analysis used to confirm the payloads behavior? |

Reflections/Notes:

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

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

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

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

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. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it really fascinating 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.

---

## 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.