**Incident handler's journal**

| **Date:** March 1, 2025 | **Entry:** #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | None | | |
| The 5 W's | * **Who:** An organized group of unethical hackers. * **What:** A ransomware security incident * **When:** Tuesday 9:00 a.m. * **Where:** A healthcare company * **Why:** The incident occurred when unethical hackers infiltrated the company's systems through a phishing attack. Once inside, they deployed ransomware, encrypting critical files. Their primary motive appears to be financial, as evidenced by the ransom note demanding a significant payment for the decryption key. | | |
| Additional notes | The healthcare company can prevent future attacks by training employees, enhancing email security, enforcing MFA, using threat detection tools, updating software, segmenting networks, maintaining offline backups, and having an incident response plan.  Paying the ransom is discouraged due to risks like no guarantee of recovery, encouraging more attacks, and potential legal issues. Instead, the company should restore from backups, seek cybersecurity expertise, and report the incident to authorities. | | |

| **Date:** March 2, 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, a network protocol analyzer with a graphical interface, is valuable in cybersecurity as it enables security analysts to capture and examine network traffic, aiding in the detection and investigation of malicious activity. | | |
| The 5 W's | * **Who:** N/A * **What:** N/A * **When:** N/A * **Where:** N/A * **Why;** N/A | | |
| Additional notes | I had never used Wireshark before, so I was excited to dive into this exercise and analyze a packet capture file. At first, the interface felt overwhelming, but I quickly realized why it's such a powerful tool for understanding network traffic. | | |

| **Date:** March 3, 2025 | **Entry:** #3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. Like Wireshark, tcpdump helps security analysts capture, filter, and analyze network traffic. | | |
| The 5 W's | * **Who:** N/A * **What:** N/A * **When:** N/A * **Where:** N/A * **Why:** N/A | | |
| Additional notes | I'm still new to the command-line interface, so capturing and filtering network traffic was challenging. I got stuck a few times due to incorrect commands, but after carefully following instructions and redoing some steps, I successfully completed the activity. | | |

| **Date:** March 4, 2025 | **Entry:** #4 | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | For this activity, I used VirusTotal, an investigative tool that scans files and URLs for malicious content like viruses, worms, and trojans. It’s great for quickly checking if an indicator of compromise, such as a file or website, has been flagged by the cybersecurity community.  I analyzed a file hash in VirusTotal, which was reported as malicious. This incident took place during the Detection and Analysis phase, where I acted as a SOC security analyst investigating a suspicious file hash. After the security system flagged the file, I conducted further analysis to determine whether it posed 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 * **When:** An employee's computer at a financial services company * **Where:** 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 | To prevent this type of incident in the future, the organization should enhance email security with advanced filtering and attachment scanning, implement endpoint protection to detect and block threats, enforce least privilege access to limit damage, and regularly update security policies.  Improving security awareness training is also crucial. Employees should be educated on identifying phishing emails, verifying attachments, and reporting suspicious activity to reduce the risk of human error. | | |

| **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. | | |

### 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:  I found using tcpdump particularly challenging. Since I'm new to the command line, learning its syntax was a steep learning curve. Initially, I felt frustrated because I wasn’t getting the right output. However, after redoing the activity and carefully following the instructions, I identified my mistakes. This experience taught me the importance of patience and attention to detail.  My understanding of incident detection and response has significantly improved throughout this course. At first, I had a basic grasp of the concepts, but I didn’t fully appreciate the complexity involved. As I progressed, I learned about the incident lifecycle, the role of structured processes, and the tools used for detection and response. Now, I feel more confident in my knowledge and ability to apply these concepts.  I really enjoyed network traffic analysis, especially using network protocol analyzer tools. It was my first time exploring this topic, making it both challenging and exciting. Capturing and analyzing network traffic in real-time was fascinating, and it sparked my interest in learning more. I hope to continue building my skills and become proficient in using these tools. |
| --- |