**Incident handler's journal**.

|  |  |
| --- | --- |
| **Date:**  09 April 2025 | **Entry: RW000001**  Record the journal entry number. |
| Description | Around 9:00 AM, employees reported being locked out of their files and medical records. Their desktops displayed a ransom note stating that files were encrypted by hackers demanding money for the decryption key. This ransomware attack originated from phishing emails sent to multiple employee accounts. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** A group of unethical hackers * **What** Ransomware attack * **When** Tuesday at 9 AM. * **Where?** At a healthcare company * **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? |

|  |  |
| --- | --- |
| **Date:**  9th April 2025 | **Entry: RW000002**  Record the journal entry number. |
| 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 | Capture the 5 W's of an incident.   * **Who** caused the incident? N/A * **What** happened? N/A * **When** did the incident occur? N/A * **Where** did the incident happen? N/A * **Why** did the incident happen? N/A |
| Additional notes | I've never worked with Wireshark previously, so I was eager to start this exercise and examine a packet capture file. At a first look, the interface seemed quite understandable. I understand why it's an effective instrument for analyzing network traffic |

|  |  |
| --- | --- |
| **Date:**  9th April 2025 | **Entry: RW000003** |
| Description | Capturing my first packet |
| Tool(s) used | In this task, I utilized tcpdump to record and examine network traffic. Tcpdump is a command-line interface tool used to analyze network protocols. Like Wireshark, the importance of tcpdump in cybersecurity lies in its ability to enable security analysts to capture, filter, and examine network traffic. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? N/A * **What** happened? N/A * **When** did the incident occur? N/A * **Where** did the incident happen? N/A * **Why** did the incident happen? N/A |
| Additional notes | Since I'm still inexperienced with the command-line interface, using it to capture and filter network traffic proved to be difficult. I encountered difficulties a few times due to using incorrect commands. However, by meticulously adhering to the guidelines and repeating certain steps, I managed to complete this task and record network traffic. |

|  |  |
| --- | --- |
| **Date:**  10th April 2025 | **Entry: Entry: RW000004** |
| Description | Investigate a suspicious file hash |
| Tool(s) used | Tool(s) utilized For this task, I employed VirusTotal, which is a research tool that examines files and URLs for harmful content like viruses, worms, trojans, and others. It's a highly useful resource for swiftly verifying whether an indicator of compromise, such as a file or website, has been flagged as malicious by members of the cybersecurity community. In this task, I utilized VirusTotal to examine a file hash that was flagged as harmful.  This event took place during the Detection and Analysis stage. The situation placed me in the role of a security analyst at a SOC examining a dubious file hash. Once the security systems identified the suspicious file, I needed to conduct a more thorough analysis and investigation to ascertain whether the alert indicated a genuine threat. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** An unknown malicious actor. * **What** An email sent to an employee contained a malicious file attachment that was executes once it was opened with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When** At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Where** An employee's computer at a financial services company * **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/Notes: Record additional notes.   1. **Were there any specific activities that were challenging for you? Why or why not?**   The tcpdump activity proved to be quite difficult for me. I'm new to using the command line, so learning the syntax for a tool like tcpdump was a steep learning curve. At first, I was very frustrated because I wasn't getting the desired results. I redid the activity and discovered where I went wrong. This taught me to read the instructions carefully and take my time with the process.   1. **Has your understanding of incident detection and response changed after taking this course?**   After taking this course, my comprehension of incident detection and response has greatly improved. At the start of the course, I had a basic concept of what detection and response include, but I didn't fully grasp the complexities. As I moved through the training, I learned about the incident lifecycle, the importance of planning, processes, and people, and the tools that were employed. Overall, I believe my understanding has improved, and I am now better positioned to notice and respond to incidents.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   I thoroughly loved studying about network traffic analysis and applied what I learned using network protocol analyzer tools. It was my first experience learning about network traffic analysis, so it was both tough and intriguing. I thought it was amazing to be able to use technologies to record and analyze network data in real time. I am definitely more interested in learning more about this subject, and I hope to one day become more skilled in the use of network protocol analyzer software. |