**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:**  Record the date of the journal entry. | **Entry: #1**  **January Tuesday 9:00 am** |
| 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.   **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.  Documenting a cybersecurity incident. Employee downloaded a spreadsheet that had a malicious payload attached |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An organized group of unethical hackers * **What:** A ransomware security incident * **When:** Tuesday at 9:00 am * **Where:** At a small U. S. Health care clinic * **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 and encrypted critical files. The attacker’s 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:**  Record the date of the journal entry. | **Entry: 2**  **July 25th 1:11pm** |
| Description | Analyze your first packet |
| 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.   * **What:** opened saved packet capture files, viewed high-level packet data, and used filters to inspect detailed packet data * **When:** at 1:11pm July 25th 2024 * **Where:** on desktop used wire shark to inspect data packet * **Why:** to check for any suspicious transactions. |
| Additional notes | On a desktop used wire shark to gain some experience opening a saved packet of captured files. Viewed high-level packet data and used filters to inspect detailed packet data. Used basic Wireshark filter and inspected a packet, which provided details about the overall network packet including the frame length and the arrival time of the packet. Used filters to select packets. Use filters to explore DNS packets. Use filters to explore TCP packets.  It was my first time using Wireshark, there is a lot to it and I am happy to learn how to use new program. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 3**  **August 1st 1:11 pm** |
| Description | Capturing my first packet. Analyze live network traffic from Linux virtual machine |
| 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 | Capture the 5 W's of an incident.   * **What:** identify network interfaces * **When:** at 1:11pm * **Where:** using Linux * **Why:** captured network traffic with tcpdump, identify network interfaces, using tcpdump command to capture network data for inspection, interpret the information that tcpdump outputs regarding a packet, and save and load packet data for later analysis |
| Additional notes | captured network traffic with tcpdump, identify network interfaces, using tcpdump command to capture network data for inspection, interpret the information that tcpdump outputs regarding a packet, and save and load packet data for later analysis  I like using the command-line interface, this exercise I was able to capture and filter network traffic. This was a good experience. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 4**  **September 14th 1:20 pm** |
| Description | 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.  Investigate a suspicious file hash. 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:** 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:** at 1:20pm 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. This happened because the employee downloaded an infected spreadsheet without doing a scan of the file before downloading or opening the file. |
| Additional notes | This file is rated 60/73 on the virus total site as a security risk by vendors and 3 sandboxes flagged this file as malicious  It falls into the category as a Trojan  Creation date 2020-09-14 – 01:13:36 UTC  The Hash was detected as malicious  Intrusion software was alerted  Multiple unauthorized executable files are created on the employee’s computer  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? |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 5**  **October 1st 2:30 pm** |
| Description | Examine alerts, logs and rules |
| Tool(s) used | suricata |
| The 5 W's | Capture the 5 W's of an incident.   * **What** Create custom rules and run them in Suricata, monitor traffic captured in a packet capture file and examine the fast.log and eve.json output |
| Additional notes | Create custom rules and run them in Suricata, monitor traffic captured in a packet capture file and examine the fast.log and eve.json output |

|  |  |
| --- | --- |
| **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. |