**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:**  2025-07-01 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Analyzed a suspicious email attachment and confirmed it was a phishing attempt using VirusTotal. This activity falls under the 'Detection and Analysis' phase of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | **VirusTotal, Email client** | | |
| The 5 W's | Capture the 5 W's of an incident.  **The 5 W's:**  **- Who caused the incident? A malicious external actor**  **- What happened? Phishing email with malicious attachment**  **- When did the incident occur? July 1, 2025**  **- Where did the incident happen? Company's email system**  **- Why did the incident happen? Attempt to gain unauthorized access to internal resources**  **Additional Notes: This entry demonstrates practical detection of a common attack vector.** | | |
| Additional notes | This entry demonstrates practical detection of a common attack vector. | | |

| **Date:**  2025-07-03 | **Entry:**  **1** | | |
| --- | --- | --- | --- |
| Description | Used Wireshark to capture network packets during a simulated attack. This exercise aligns with the 'Preparation' and 'Detection and Analysis' phases. | | |
| Tool(s) used | **Wireshark** | | |
| The 5 W's | Capture the 5 W's of an incident.  **The 5 W's:**  **- Who caused the incident? Red team during simulation**  **- What happened? Network scan and reconnaissance**  **- When did the incident occur? July 3, 2025**  **- Where did the incident happen? Internal network lab**  **- Why did the incident happen? To identify vulnerable systems** | | |
| Additional notes | Packet analysis was critical in identifying unusual ARP traffic. | | |

| **Date:**  2025-07-06 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Performed a query in Splunk to identify login anomalies. This activity supports the 'Detection and Analysis' and 'Containment' phases. | | |
| Tool(s) used | **Splunk** | | |
| 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 | Query syntax understanding improved during this task. | | |

| **Date:**  2025-07-08 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Explored Suricata logs to detect suspicious signature-based traffic patterns. This activity aligns with the 'Detection and Analysis' phase. | | |
| Tool(s) used | **Suricata** | | |
| 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 | Valuable experience in working with IDS tools and understanding signatures. | | |

| **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. | | |

| **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:  1. One of the more challenging activities was analyzing Suricata logs due to the volume and complexity of signatures. It required close attention to detail and repeated practice to interpret patterns effectively.  2. My understanding of incident detection and response has significantly improved. I now better understand the NIST IR phases and how to use tools like Splunk and Wireshark to detect and analyze threats.  3. I particularly enjoyed using Wireshark. It provided real-time insights into network activity and helped me visually trace suspicious behaviors across a session. |
| --- |