**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** | | |
| --- | --- | --- | --- |
| Description | A small U.S. health care clinic experienced a ransomware attack on a Tuesday morning at 9 am. Employees couldn't access files due to encryption and a ransom note demanded money for decryption. The attackers used phishing emails with malicious attachments to gain access. Patient data was compromised, operations disrupted, and the clinic sought technical help. | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** group of unethical hacker * **What** send phishing message included ransomware * **When** tuesday 9 am * **Where** U.S. health care clinic * **Why** attackers send phishing messages included ransomware to several employees in the company. Their motive is to get money so they can give the decryption key to the clinic | | |
| 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** | | |
| --- | --- | --- | --- |
| Description | Analyzing packet capture file | | |
| Tool(s) used | In this lab, I used wireshark to analyze a captured file. By learning and implementing commands to find essential information, I can detect and and investigate malicious activities | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**? 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 | At first, I find it difficult to understand and implement with it, but after learning all commands and its functionalities, I find it very interesting and convenient for analyzing and investigating | | |

| **Date:**  Record the date of the journal entry. | **Entry: #3** | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | In this lab, I used tcpdump to capture and analyze network traffic. I have an opportunity to apply all theories about tcpdump that I’ve learned from videos into a practical lab. Therefore, now I know how to capture network traffic with different options. | | |
| 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 just know the basic of capturing network traffic and display network capture file in the terminal, but I haven’t got analyzing skills from doing tcpdump | | |

| **Date:**  Record the date of the journal entry. | **Entry: #4** | | |
| --- | --- | --- | --- |
| Description | An employee downloaded and opened a malicious file from a phishing email. The sender's email address, name in the email body, and sender's name are inconsistent. The email had grammatical errors, and it contained a password-protected attachment named "bfsvc.exe." This attachment was confirmed to be a known malicious file. The alert severity was medium. The situation has been escalated to a level-two SOC analyst for further action. | | |
| Tool(s) used | In this lab, I used Virustotal to investigate a SHA-256 hash file. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? attacker * **What** happened? An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When** did the incident occur? 1:20pm * **Where** did the incident happen? In the company * **Why** did the incident happen? A employee downloads the bfsvc.exe file | | |
| Additional notes | How can we prevent this in the future?  How did it get contained? | | |

| **Date:**  Record the date of the journal entry. | **Entry: #5** | | |
| --- | --- | --- | --- |
| Description | Investigate failed login attempts in email server of e-commerce store Buttercup Games | | |
| Tool(s) used | In this lab, I used Splunk to query failed SSH login events and investigate it. I’ve learned how to upload, query data and narrow down search methods in order to speed up my query to achieve results. | | |
| 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 | So far, I haven’t discovered any suspicious activity while querying with Splunk, but I just know some basic command to query. | | |

| **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: Record additional notes. |
| --- |