**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:**  February 12th, 2025 | **Entry:**  001 | | |
| --- | --- | --- | --- |
| Description | A small U.S clinic experienced a security incident that disrupted their business operations. The incident was caused by a phishing email that had a ransomware attachment that hackers used to encrypt company files. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Unethical Hackers targeted the organization.** * **Employees were not able to access files such a medical records which shut down business operations as those files are needed to do their jobs.** * **The incident occurred on Tuesday at 9:00 am** * **The incident took place virtually on the company’s network.** * **The hackers sent phishing emails to the employees and when the attachment was downloaded it granted them access to the files which they then encrypted.** | | |
| Additional notes | How can this be prevented in the future? | | |

| **Date:**  February 14th, 2025 | **Entry:**  002 | | |
| --- | --- | --- | --- |
| Description | Responding to a phishing alert using a playbook | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | * Someone on the HR team opened a email attachment that has a file hash that has been verified as malicious * This incident occurred on Wednesday, July 20, 2022 09:30:14 * Online via email * This incident happened as a attached file, which was malicious, was downloaded | | |
| Additional notes | After doing my investigation I have escalated the ticket and notified a level two SOC analyst. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su’” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. | | |

| **Date:**  February 15th, 2025 | **Entry:**  003 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | I analyzed a packet capture file using Wireshark, a network protocol analyzer with a graphical user interface. Wireshark 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 | 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 | Having never used Wireshark before this was an eye opening experience. The interface was quite overwhelming at first, but I can see why it's such a powerful tool for analyzing network traffic. I look forward to gaining more experience with it. | | |