**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:**  September 20, 2024 | **Entry:**  # 1 |
| Description | Small U.S health care clinic security incident |
| Tool(s) used | None |
| The 5 W's | * **Who:** Organized Unethical Hackers who are known to target healthcare and transportation services. * **What:** Emails had malware which included ransomware, in turn all of the companies’ files were encrypted. * **When:** Tuesday Morning, at approximately 9:00 am. * **Where:** In a Small U.S healthcare clinic which specializes in delivering primary-care services. * **Why:** Because of targeted phishing emails which the employees were unaware of. |
| Additional notes | * The company most likely does not have a risk management plan or an incident management plan in place. * The company does not have a CSIRT team to manage a security incident, they had to result to third-party organizations to handle their security incident. |

|  |  |
| --- | --- |
| **Date:**  September 23, 2024 | **Entry:**  # 2 |
| Description | Hash file investigation |
| Tool(s) used | VirusTotal |
| The 5 W's | * **Who**: An advanced threat actor called BlackTech. * **What**: This advanced threat actor created a malware called Flagpro. * **When**: The malware was first seen on February 15, 2020. * **Where**: Targeted countries such as Taiwan, Japan and English-Speaking countries. * **Why**: Speculations lead to chinese-state backed hackers. |
| Additional notes | <https://www.bleepingcomputer.com/news/security/new-flagpro-malware-linked-to-chinese-state-backed-hackers/>  <https://www.virustotal.com/gui/file/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/>  https://malpedia.caad.fkie.fraunhofer.de/details/win.flagpro |

|  |  |
| --- | --- |
| **Date:**  September 21, 2024 | **Entry:**  # 3 |
| Description | Analyzing packets with Wireshark |
| Tool(s) used | Wireshark |
| The 5 W's | The 5 W’s is not applicable  I learned about:   * Saved packet capture files * Opening saved packet capture files * View packet data * Filters to inspect packet data |
| Additional notes | I used these lab activities by google:  <https://www.cloudskillsboost.google/focuses/38337603?parent=lti_session>  https://www.cloudskillsboost.google/focuses/38337265?parent=lti\_session |

|  |  |
| --- | --- |
| **Date:**  September 21, 2024 | **Entry:**  # 4 |
| Description | Capturing packets with tcpdump |
| Tool(s) used | tcpdump |
| The 5 W's | The 5 W’s is not applicable  I learned about:   * How to identify network surfaces * How to use tcpdump to capture network data * Interpret information that tcpdump outputs * Save and load packet data for analysis |
| Additional notes | I used these lab activities by google:  https://www.cloudskillsboost.google/focuses/38337646?parent=lti\_session  https://www.cloudskillsboost.google/focuses/38337616?parent=lti\_session |

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