**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:** 10/31/2023 | **Entry: 1** |
| Description | A small U.S. health clinic encountered a security incident where they selected a phishing email without expecting a malicious attachment. Once the attachment was downloaded, their devices opened a ransomware attack encrypting their personal files and demanded payment. |
| Tool(s) used | None**.** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**? The hackers. * **What**? The hackers implemented ransomware on the health clinics software, encrypting the organization’s computer files. * **When**? It occurred on Tuesday at 9:00 a.m.. * **Where**? It occurred at a small health clinic in the United States. * **Why**? The hackers wanted money from the health clinic. |
| Additional notes | Should the company pay the ransom to receive the decryption key or is there a better solution?  How could the healthcare company prevent these incidents from occurring again? |

|  |  |
| --- | --- |
| **Date:**  11/5/2023 | **Entry:**  2 |
| Description | An employee has encountered a phishing incident. |
| Tool(s) used | Input Capture |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Threat Actor   * **What** happened?   An employee opened a password-protected spreadsheet file and was immediately compromised.   * **When** did the incident occur?   1:13 P.M.   * **Where** did the incident happen?   At a financial services company.   * **Why** did the incident happen?   The threat actor wanted to implement malicious payload to the device to steal any confidential messages. |
| Additional notes | How legitimate and trustworthy did the email turn out to be to trick the employee?  What is the best immediate to take after a malicious payload? |

|  |  |
| --- | --- |
| **Date:**  11/5/2023 | **Entry:**  3 |
| Description | An individual gained unauthorized access to personable identifiable information and financial information. |
| Tool(s) used | Routine vulnerability scans and penetration testing. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   A vulnerability in the e-commerce web application caused by the attacker.   * **What** happened?   The attacker performed a forced browsing attack and accessed customer transaction data by modifying the order number included in the URL string of  a purchase confirmation page. The attacker accessed customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.   * **When** did the incident occur?   It occurred on December 28, 2022 at 3:13 P.M..   * **Where** did the incident happen?   At an unknown organization.   * **Why** did the incident happen?   The attacker committed these attacks to steal large amounts of money from customers. |
| Additional notes | What is the best way to prevent a forced browsing attack? |

|  |  |
| --- | --- |
| **Date:**  11/6/2023 | **Entry:**  4 |
| Description | Identifying a phishing email with a suspicious domain. |
| Tool(s) used | Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   The hackers   * **What** happened?   The hackers send multiple phishing emails to employees of a financial organization, causing them to press the malicious domain.   * **When** did the incident occur?   Occurred on July 1 at 2;32 PM.   * **Where** did the incident happen?   At a financial services industry.   * **Why** did the incident happen?   The attackers want to steal confidential login credentials. |
| Additional notes | Include any additional thoughts, questions, or findings.  There should be a training program for new employees to learn about phishing emails and determining if a domain is suspicious. Implementing this program will help reduce any phishing incidents. |

|  |  |
| --- | --- |
| **Date:**  11/6/2023 | **Entry:**  5 |
| Description | Working as a security analyst to discover any failed login attempts. |
| Tool(s) used | Splunk |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Attackers   * **What** happened?   The attackers tried logging in to the mail server without permission.   * **When** did the incident occur?   November 10th at 4:32 PM.   * **Where** did the incident happen?   At a e-commerce store called Buttercup Games.   * **Why** did the incident happen?   The attackers tried obtaining the sensitive data from the mail server for their own benefit. |
| Additional notes | Include any additional thoughts, questions, or findings.  What exactly would the attackers do if they successfully infiltrated the data from the mail server? |

|  |  |
| --- | --- |
| **Date:** 11/6/2023 | **Entry: 6** |
| Description | Analyzing a packet capture file. |
| 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.  Who: N/A  ● What: N/A  ● Where: N/A  ● When: N/A  ● Why: N/A |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and  analyze a packet capture file. At first glance, the interface was very  overwhelming. I can see why it's such a powerful tool for understanding  network traffic. |

### 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.  **1. Were there any specific activities that were challenging for you? Why or why not?**  I really found the activity using tcpdump challenging. I am new to using the command line, and  learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated  because I wasn't getting the right output. I redid the activity and figured out where I went wrong.  What I learned from this was to carefully read the instructions and work through the process  slowly.  **2. Has your understanding of incident detection and response changed after taking**  **this course?**  After taking this course, my understanding of incident detection and response has definitely  evolved. At the beginning of the course, I had some basic understanding of what detection and  response entailed, but I didn't fully understand the complexity involved. As I progressed through  the course, I learned about the lifecycle of an incident; the importance of plans, processes, and  people; and tools used. Overall, I feel that my understanding has changed, and I am equipped  with more knowledge and understanding about incident detection and response.  **3. Was there a specific tool or concept that you enjoyed the most? Why?**  I really enjoyed learning about network traffic analysis and applying what I learned through  network protocol analyzer tools. It was my first time learning about network traffic analysis, so it  was both challenging and exciting. I found it really fascinating to be able to use tools to capture  network traffic and analyze it in real time. I am definitely more interested in learning more about  this topic, and I hope to one day become more proficient in using network protocol analyzer  tools. |