**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:** 22/04/2024 | **Entry: #1** |
| Description | Documenting a ransomware incident. |
| Tool(s) used | Encryption |
| The 5 W's | Capture the 5 W's of an incident.   * The incident was caused by an organized group of unethical hackers. * The hackers encrypted company systems including critical medical record using ransomware. * The incident occurred on 22nd April 2024. * The incident happened at a small healthcare clinic. * The attackers targeted company employees using a phishing campaign. They compromised the system’s defenses when an unsuspecting employee clicked on the link which installed malware on their computer. They happened to gain access across the network to more critical data. Eventually sensitive medical records were encrypted using ransomware. The attack seems to have been financially motivated because they demanded a large sum of money be paid to them for the decryption key. |
| Additional notes | What effect do antiviruses have on ransomware. Is it possible that an antivirus can stop the installation and execution of malware? How did they get the emails of the company’s employees? |

|  |  |
| --- | --- |
| **Date:** 29/04/2024 | **Entry: #2** |
| Description | Investigating a phishing incident |
| Tool(s) used |  |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The incident was cause by a malicious actor who sent a phishing link via an email to one of the HR staff. * **What** happened? The staff viewed the email and clicked on the link which downloaded a malware to their personal computer and ran some executables on their local PC. * **When** did the incident occur? The incident occurred at 1:13pm when the employee successfully downloaded and opened the file. * **Where** did the incident happen? The incident occurred at a financial services company. * **Why** did the incident happen? An unsuspecting employee click on a phishing link which downloaded a malware on their PC. |
| Additional notes | Include any additional thoughts, questions, or findings.  The additional information page shows that the email contained numerous grammar and spelling errors( Ingergy, writing for to express, posted from the website, there is attached my resume ) as well as an executable file which was attached with the email. The domain name of the email also looked suspicious. |

|  |  |
| --- | --- |
| **Date:** 28/12/2022 | **Entry: #3** |
| Description | Reviewing a Incident Final Report |
| Tool(s) used |  |
| The 5 W's | Capture the 5 W's of an incident.   * An attacker gained unauthorized to customer data through the purchase confirmation page on an ecommerce website. * Approximately 50,000 customer records were exfiltrated from the organization’s ecommerce site. The attacker gained access by performing a forced browsing attack and modifying the order number included in the URL string of a purchase confirmation page. * The incident occurred on December 22, 2022, at 3:13 P.T. * The incident happened at a mid-sized retail company. * Theincident happened due to an unpatched vulnerability in the company’s e-commerce web application. |
| Additional notes | How did the attack exfiltrate the data from the site. Why was the exceptionally high volume of sequentially listed customer orders not detected by the company’s defense systems? Why were the company not carrying out penetration testing prior to the event? |

|  |  |
| --- | --- |
| **Date:** 08/05/2024 | **Entry: #4** |
| Description | Exploring Failed SSH Logins For a Root Account |
| Tool(s) used | **SPLUNK CLOUD** |
| The 5 W's | * A malicious actor making multiple attempts to log into the system using root user credentials. * This event happened on the 6th of March 2023 |
| Additional notes | Over 300 failed SSH root login logs were captured by Splunk which is an indicator of a malicious attempt by a threat actor to compromise root user SSH credentials. The request originated from multiple IP addresses. |

|  |  |
| --- | --- |
| **Date:** | **Entry: #5** |
| Description | Investigating a Phishing Event. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | * A threat actor sent a phishing email to different employees in the company. * Log records show that several assets within the company have accessed and interacted with the domain. * The incident was first spotted on the 31st of January 2023. * The incident took place at a financial services company. * Several employees had already visited the malicious domain. |
| Additional notes | 12 different assets accessed the domain on January 31st and July 9th respectively. The assets are ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc, and warren-morris-pc.  Assets that made HTTP **POST** requests to the domain.   1. Ashton-davidson-pc 31/01/2023 2. Emil-palmer-pc 31/01/2023 3. Warren-morris-pc 31/01/2023   Associated Domains  Signin.accounts-gooqle.com  Signin.office365x24.com |

|  |  |
| --- | --- |
| **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. |