**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:**  10/04/2024 | **Entry: 1** |
| Description | A small health care provider in the U.S.A. experienced a security incident that completely disrupted business continuity. |
| Tool(s) used | **NO TOOLS WERE USED** |
| The 5 W's | * **Who** caused the incident? A group of unethical hackers that target the healthcare and transportation industries. * **What** happened? Through spear phishing the malicious actors were able to gain access to the company data and encrypt it, to then send a ransom monetary request to provide the decryption key. This security incident is called a Ransomware attack. * **When** did the incident occur? The incident occurred on Tuesday at 9:00 a.m. * **Where** did the incident happen? The incident happened in a small health care provider in the U.S.A. * **Why** did the incident happen? The cause of the incident was a successful spear phishing attack. This means that one or more targeted employees unwillingly gave access to the threat actors. |
| Additional notes | To avoid further incidents like this, it is recommended to encrypt the company’s data in the three states of data, apply stronger password policies, enforce the principle of least privilege and separation of duties, and finally, increase employee training to detect and report these incidents. |
|  |  |

|  |  |
| --- | --- |
| **Date:**  11/04/2024 1:20 p.m. | **Entry: 2** |
| Description | An IDS detected an employee downloading and executing a file from an email. |
| Tool(s) used | Suricata and Linux commands |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An employee unknowingly downloading a malicious file * **What** happened? The employee downloaded a file that was executed via a password given as a pretense to open the document. * **When** did the incident occur?   1:11 p.m.: An employee receives an email containing a file attachment.  1:13 p.m.: The employee successfully downloads and opens the file.  1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.  1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.   * **Where** did the incident happen? In the employee’s work computer. * **Why** did the incident happen? Because there wasn’t enough awareness about social engineering attacks, email filters and lack of user restrictions to download and execute files. |
| Additional notes | The company must do more awareness campaigns and install filters. Also, the principle of least privilege must be more strongly enforced, |

|  |  |
| --- | --- |
| **Date:** 12/04/2024  10:04 a.m. | **Entry: 3** |
| Description | An employee of a small financial services company received a phishing email with a high risk downloadable file. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A ‘Clyde West’, probably a malicious actor impersonating a real person. * **What** happened? Said person sent an email expressing interest to work in the company, so a password protected ‘CV’ named ‘bsfc.exe’ was attached to the mail. * **When** did the incident occur? The incident occurred in 12/04/2024 * **Where** did the incident happen? In the company’s premises * **Why** did the incident happen? The incident happened because a supposed ‘job application’ bypassed the email filters. |
| Additional notes | The company must ensure that execution permits are in accordance to the least privilege principle. Also, even more awareness campaigns to detect and report more phishing attacks. |

|  |  |
| --- | --- |
| **Date:**  12/04/2024 11:40 a.m. | **Entry: 4** |
| Description | An unauthorized user gained access to PII and financial information of the company, which incurred in heavy financial losses and reputational damage. |
| Tool(s) used | Wireshark and tcpdump |
| The 5 W's | * **Who** caused the incident? An unauthorized user * **What** happened? The threat actor exploited a vulnerability in the e-commerce web application to gain access to customer purchase confirmation pages and exfiltrate the data, by performing a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. * **When** did the incident occur? December 22 2022 at 3:13 p.m. (PT) * **Where** did the incident happen? The incident happened in an employees work on a computer in company premises. * **Why** did the incident happen? Lack of access control mechanisms and regular vulnerabilities assessments including pen testing. |
| Additional notes | I had no idea about those types of vulnerabilities.  Must be prepared for anything. |

|  |  |
| --- | --- |
| **Date:**  15/04/2024 | **Entry: 5** |
| Description | Possible successful phishing attack |
| Tool(s) used | Chronicle and SPLUNK |
| The 5 W's | * **Who** caused the incident? One or more employees that clicked a malicious link on an email from the IP 40.100.174.34. * **What** happened? Possible data exfiltration * **When** did the incident occur? A year ago * **Where** did the incident happen? Employee work computer * **Why** did the incident happen? Not enough awareness campaigns and lack of filtering |
| Additional notes | At 14:10 on 2023-01-31 ‘ashton-davidson-pc’ signed in to the malicious link and and the POST flag suggests a successful phishing attempt, likewise other devices are possible compromised.  The Ip is associated with two domains: ‘signin.accounts-gooqle.com’ and ‘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:  The most challenging aspects of the activities were by far the amount of command and syntax that I had to familiarize myself with, to properly assess and document incidents. Although, it could have been worse if not for my previous knowledge of Python and SQL.  My understanding of incident response has changed a lot, since now I get to truly express, comprehend and react to threats in more technical terms.  I especially loved the amount of Linux labs, since it is one of the tools that has me more interested to learn more. I just like to type commands and look at the interface, as well as the results of said commands. |