**Incident handler's journal**

| **Date:**  10/16/2023 | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | Incident report for a possible ransomware attack initiated through spear phishing. | | |
| Tool(s) used | NONE | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: A group of unethical hackers * **What**: A ransomware was deployed through a spear phishing attack. * **When:** 9:00 Am Tuesday * **Where**: At a health care company. * **Why**: The incident happened because a group of hackers executed a targeted phishing attack and successfully infiltrated the healthcare company’s system. This breach allowed them to infect the system with ransomware. | | |
| Additional notes | To prevent a similar incident from occurring again, the healthcare company could implement the following measures:   * Conduct **security training** for employees to enhance their ability to identify and avoid phishing attacks. * Utilize **Intrusion Detection Systems (IDS)** or **Intrusion Prevention Systems (IPS)** to monitor and protect the network from potential threats. * Maintain a **backup server** to ensure data availability in case of any possible attack. | | |

| **Date:**  10/17/2023 | **Entry:**  #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture | | |
| Tool(s) used | Wireshark - an open-source packet and network protocol analyzer with a graphical user interface. It allows security analysts to capture, filter, and analyze network traffic. | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:** July 25 2024 | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | Tcpdump - a network protocol analyzer that's accessed using the command-line interface. It is similar to Wireshark, it allows security analysts to capture, filter, and analyze network traffic. | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes | I was able to get through this activity and capture network traffic. | | |

| **Date:**  10/18/2023 | **Entry:**  #4. | | |
| --- | --- | --- | --- |
| Description | Investing incident report on a malware download on an employees system through a phishing email | | |
| Tool(s) used | Sha256 - to hash suspicious file that was downloaded file to the system  VirusTotal - to analyze suspicious file hash | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** A employee who downloaded a malicious file * **What**: Malicious attachment from a phishing email with the hash file 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When**: 1:15 p.m * **Where:**  at work on an employee's computer. * **Why**: A malicious file was downloaded and it executed itself. | | |
| Additional notes | To prevent a similar incident from occurring again,   * Conduct **security training** for employees to enhance their ability to identify and avoid phishing attacks. * Utilize **Intrusion Detection Systems (IDS)** or **Intrusion Prevention Systems (IPS)** to monitor and protect the network from potential threats. | | |

| **Date:**  10/22/2023 | **Entry:**  #5. | | |
| --- | --- | --- | --- |
| Description | Investing any failed SSH logins for the root account to identify whether there are any possible security issues with the mail server at the e-commerce store Buttercup Games. | | |
| Tool(s) used | Splunk - monitor, investigate and analyze Buttercup Games security logs | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An unknown threat actor * **What:** An unsuccessful brute force attack * **When:** Occurred repeatedly at 1:38AM from 2/27/2023 to 3/6/2023 at 1:38AM * **Where**: on the company mail server * **Why**: A threat actor was attempting to gain unauthorized access to Butter Gamers mail server through a brute force attack. | | |
| Additional notes | Utilize **Intrusion Detection Systems (IDS)** to monitor the network from potential threats.  Set an authentication policy to lock accounts after X number of failed password login attempts. | | |

| **Date:**  10/25/2023 | **Entry:**  #6 | | |
| --- | --- | --- | --- |
| Description | Investigating possible phishing from an email sent from **signin.office365x24.com**  to an employee email | | |
| Tool(s) used | Chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: employee who open email from a threat author outside the organization * **What**: Data was sent via **POST** from the employees endpoint to the **signin.office365x24.com** domain * **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. | | |

| **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.   1. Were there any specific activities that were challenging for you? Why or why not?   Using splunk and chronicle, there is so much information you do not know where to look,   1. Has your understanding of incident detection and response changed since taking this course?   Yes , very much so.   1. Was there a specific tool or concept that you enjoyed the most? Why?   Hashing, this fact the same file will always create the same hash unless altered. |
| --- |