**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** 04/11/2024 | **Entry: #1** |
| Description | Documenting a cyber security incident |
| Tool(s) used | None |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: Ransomware security incident occurred * **When**: 9:00am Tuesday * **Where**: Healthcare clinic * **Why**: The incident happened due to unethical hackers gaining access to the company systems using a phishing attack. After the hackers gained access to the system, the attackers launched their own ransomware attack encrypting sensitive company files and data. This attack seems to be financially motivated as they left an note demanding money in exchange for a decryption key. |
| Additional notes | 1. How can the company take preventive measures to ensure that an incident like this will not occur again? 2. Should the company pay the ransom to receive a decryption Key |

|  |  |
| --- | --- |
| **Date:** 07/11/2024 | **Entry: #2** |
| Description | Analyzing a Packet Capture |
| Tool(s) used | For this activity, the tool used was 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 | * **Who**: Malware * **What**: Malware was executed from a corrupt file. * **When** 1:11 pm * **Where**: Financial services company on an employee’s computer. * **An** employee received an email that contained an attachment, As the employee downloaded the file and opened it, there was a malicious payload that had been executed on their computer. |
| Additional notes | 1. How can the company be better prepared next time to prevent employees from opening suspected emails? 2. Should the company prohibit personal emails from being accessed at work? |

|  |  |
| --- | --- |
| **Date:** 11/12/2024 | **Entry: #3** |
| Description | Responding to a phishing incident |
| Tool(s) used | For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.  This incident occurred in the Detection and Analysis phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| The 5 W's | * **Who**: Uknown Malicious Actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Where**: Financial service company * **Why** Employee received a malicious file from an unknown source that was disguised as a normal email. The employee proceeds to download the file not being aware of a potential malware contained inside due to the sender disguising the email as legitimate. |
| Additional notes | How can we educate employees to avoid this type of incident?  Should we prohibit employees from downloading unknown files at work? |

|  |  |
| --- | --- |
| **Date:**  11/15/2024 | **Entry: #4** |
| Description | Analyzing potential threats Using a SIEM tool |
| Tool(s) used | Splunk is a powerful SIEM tool that I used to search for threats that came from an unknown source due to many login attempt failures. |
| The 5 W's | * **Who**: web application “ww1” used by ButterCup Games * **What**: failed login attempts were reported from Splunk. * **When** 03/06/23, 6:24 pm * **Where**: Mail Server at Buttercup games * **Why**: There were over 100 login attempts from a web application by buttercup games. These failed login attempts triggered an alert and had cause to be investigated due to the potential chance of those attempts being tried by a threat actor. By using Splunk I identified that those login attempts came from a web application for the company Buttercup Games. |
| Additional notes | How can we simplify and fortify the login process for users?  Why were there so many login attempts?  Is there an authentication process involved? |

|  |  |
| --- | --- |
| **Date:**  11/15/2024 | **Entry: #5** |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, the tool used was 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.   * **N/A** * **N/A** * **N/A** * **N/A** |
| Additional notes | I have no previous experience of Wireshark, or have I used it before so it was very exciting for me to use it to analyze a packet capture file. The interface was very confusing at first, but it made sense after configuring asnd learning about it. 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:   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.   1. **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.     1. **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. |