**Incident handler's journal**

| **Date:** Jan 1, 2024 | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident  This incident occurred in the two phases:   1. **Detection and Analysis**: The scenario details the initial detection of the ransomware incident by the organization. Subsequently, the organization sought technical assistance by reaching out to multiple organization for analysis purposes. 2. **Containment, Eradication, and Recovery**:The scenario outlines the measures taken by the organization to mitigate the incident. For example, the company initiated a shutdown of their computer systems. Yet, recognizing the need for external support in combating and recovering from the incident, they reached out to several organizations for assistance. | | |
| Tool(s) used | None | | |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: A health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to gain access to the company's systems using a phishing attack.After gaining unauthorized access, the perpetrators deployed ransomware onto the organization's systems, encrypting vital files. The attackers' incentive appears to be monetary, as evidenced by the ransom note stipulating a significant payment for the decryption key. | | |
| Additional notes | 1. How could the health care company prevent this from happening again? 2. Should the company fulfill the demands of the attacker which is to pay the ransom to retrieve the decryption key? | | |

| **Date:** Jan 25 2024 | **Entry:** #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | Wireshark: A network protocol analyzer that uses a graphical user interface. | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes | A very good tool for understanding network traffic | | |

| **Date:** Jan 25 2024 | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Capturing a packet | | |
| Tool(s) used | Tcpdump | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. | | |

| **Date:** Jan 27 2024 | **Entry:**  #4 | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | 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. I also used VirusTotal to analyze a file hash, which was reported as malicious.  This incident occurred in the **Detection and Analysis** phase. The scenario positioned me as a security analyst at a Security Operations Center (SOC), tasked with investigating a suspicious file hash. Following the detection of the suspicious file by the security systems, I undertook a thorough examination and investigation to ascertain whether the alert indicated a genuine threat. | | |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. | | |
| Additional notes | How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? | | |

| 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?**   Following the completion of this course, my understanding of incident detection and response has definitely improved . I now fully understand the complexity involved in it. 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?**   This was my initial exposure to network traffic analysis, making it exhilarating. The ability to capture network traffic and conduct real-time analysis using tools was truly captivating. My interest in delving deeper into this subject has been sparked, and I aspire to enhance my proficiency in utilizing network protocol analyzer tools in the future. |
| --- |