**Incident handler's journal**

**Furkan Şen**

|  |  |
| --- | --- |
| **Date:** Sep 23, 2024 | **Entry:**  #1 |
| Description | Documenting a cybersecurity incident  This incident occurred in the two phases:   1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. |
| Tool(s) used | None |
| The 5 W's | * **Who**: An organized group of hackers * **What**: A ransomware incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? |

|  |  |
| --- | --- |
| **Date:** Sep 25, 2024 | **Entry:** #2 |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, I used 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**: - * **What**: - * **Where**: - * **When**: - * **Why**: - |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was overwhelming.  I can see why it's such a powerful tool for understanding network traffic. |

|  |  |
| --- | --- |
| **Date:** Sep 25, 2024 | **Entry:**  #3 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows us to capture, filter, and analyze network traffic. |
| The 5 W's | * **Who**: - * **What**: - * **Where**: - * **When**: - * **Why**: - |
| 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:** Sep 27, 2024 | **Entry:**  #4 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content. 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 cyber community. In this scenario, I analyzed 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**: 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. |

|  |
| --- |
| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   -   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 is, but I didn't fully understand the details involved. As I progressed through the course, I learned about the lifecycle of an incident, importance of plans, processes, tools and the people. Overall, I feel that my understanding has changed, and I am equipped with more knowledge now.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   It was my first time learning about network traffic analysis, so it was 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. |