Incident handler's journal

Andrew Beavers

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: April 18, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident occurred in two phases: 1. The organization detected the ransomware incident and sought technical assistance from several organizations for analysis**.** 2. In response to the incident, the organization took steps to contain it, such as shutting down its computer systems. However, they realized they could not handle the eradication and recovery process alone, so they sought assistance from several other organizations.
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a healthcare company • **When**: Tuesday 9:00 a.m. • **Why**: The incident occurred due to the unethical actions of hackers who were able to gain access to the company's systems through a phishing attack. Once inside, the attackers deployed their ransomware on the company's systems which encrypted important files. The attackers seemed motivated by financial gain as the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the healthcare company prevent an incident like this from

	occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: April 19 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that provides a graphical user interface. In cybersecurity, Wireshark is valuable because it allows security analysts to capture and analyze network traffic. By doing so, they can detect and investigate any malicious activity occurring on the network.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I had never used Wireshark before, so I was excited to start this exercise and analyze a packet capture file. However, the interface seemed overwhelming at first glance.

Date: April 20 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	I was eager to try this exercise and scrutinize a packet capture file. Initially, the interface appeared daunting to me, but I can comprehend why it is regarded as a robust tool for assessing network traffic.

The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I struggled with using the command-line interface to capture and filter network traffic, but after redoing some steps, I completed the activity.

Date: April 20 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	I utilized VirusTotal, which is an investigative tool that analyzes files and URLs to detect malicious content. This tool is quite helpful in quickly checking whether something has been reported as malicious. Specifically, I analyzed a hash for a reported malicious file during the Detection and Analysis phase, as part of my investigation into a suspicious file that had been flagged by the security systems in place.
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 any specific activities challenging for you? Why or why not?**

I found the activity using tcpdump quite challenging. As a beginner to command-line tools, learning the proper syntax for tcpdump was a steep learning curve for me. Initially, I felt very frustrated because I wasn't getting the desired output. However, I re-did the activity and discovered where I went wrong. From this experience, I learned the importance of carefully reading the instructions and taking the time to work through the process slowly.

2. **Has your understanding of incident detection and response changed after taking this course?**

After completing this course, my understanding of incident detection and response has significantly improved. Initially, I had a basic understanding of what incident detection and response involved, but I didn't fully comprehend the complexity of it. However, as I progressed through the course, I gained knowledge about the lifecycle of an incident, the significance of plans, processes, people, and the tools used in the process. Overall, my understanding of incident detection and response has evolved and I am better equipped with knowledge and understanding.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I enjoyed learning about network traffic analysis and using protocol analyzer tools. It was challenging and exciting. I found it fascinating to capture traffic and analyze it in real-time. I aspire to become an expert in using these tools.

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.