Incident handler's journal

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: September 5, 2023	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: The organization detected the ransomware incident and sought technical assistance from multiple organizations for analysis. 2. **Containment, Eradication, and Recovery**: To contain the incident, the company shut down their computer systems. They then contacted several other organizations for assistance in eradicating and recovering from the incident.
Tool(s) used	None
The 5 W's	• **Who**: A group of unethical hackers • **What**: Ransomware security incident • **Where**: A small U.S. health care clinic • **When**: Tuesday 9:00 a.m. • **Why**: The incident happened because unethical 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 financially 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: September 7 2023	**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**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I was new to Wireshark and eager to analyze a packet capture file. The interface initially seemed complex, but I quickly realized its power in understanding network traffic.

Date: September 8 2023	**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 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'm a beginner with the command-line interface, so capturing and filtering network traffic was tough. I made mistakes with commands a few times, but I persevered by following the instructions closely and redoing some steps until I successfully captured the network traffic.

Date: September 9 2023	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	I used VirusTotal, an investigative tool, to check if a file hash was malicious. It's handy for quickly verifying if a file or website is considered harmful by the cybersecurity community. In this case, I played the role of a security analyst in a SOC during the Detection and Analysis phase. I had to investigate a suspicious file detected by our security systems to assess if it was 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 found using tcpdump challenging initially due to my limited command line experience. I struggled with the syntax and got frustrated when the output wasn't right. However, after redoing the activity and taking it step by step, I learned the importance of reading instructions carefully and working methodically.

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

This course has significantly enhanced my grasp of incident detection and response. Initially, I had a basic understanding, but I underestimated its complexity. Through the course, I gained insights into the incident lifecycle, the significance of plans, processes, and people, as well as the tools involved. Overall, my comprehension of incident detection and response has deepened, equipping me with valuable knowledge.

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

I had a great time exploring network traffic analysis and using network protocol analyzer tools for the first time. This was a new and thrilling experience for me. The challenge was exciting, and I was captivated by the ability to capture and analyze network traffic in real-time. I'm now very keen to delve deeper into this subject and aspire to become more skilled in using network protocol analyzer tools in the future.
