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: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario details the organization's initial detection of the ransomware incident. For the analysis step, the organization sought technical assistance from several organizations. 2. **Containment, Eradication, and Recovery**: The scenario describes actions the organization took to address the incident. For instance, they shut down their computer systems. However, unable to handle the incident's eradication and recovery independently, they sought assistance from multiple other organizations.
Tool(s) used	None
The 5 W's	• **Who**: A group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident occurred when unethical hackers accessed the company's systems through a phishing attack. Upon gaining access, the attackers deployed ransomware, encrypting critical files. Their motivation seems financial, as indicated by the ransom note demanding a substantial sum in exchange for the decryption key.

Additional notes	1. How could the healthcare company prevent an incident like this from occurring again? The company can prevent this from happening again by providing regular training to employees on recognizing and avoiding phishing attacks. Also, the company can Implement email security measures, such as spam filters and email authentication protocols like SPF, DKIM, and DMARC 2. Should the company pay the ransom to retrieve the decryption key? Paying the ransom does not guarantee that the attackers will provide the decryption key, and it can also encourage further attacks

---

Date: July 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**: The User • **What**: Analyzed a packet capture file • **Where**: On WIreshark software • **When**: July 25, 2024 • **Why**: To understand network traffic and potentially detect and investigate malicious activity
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 very overwhelming. I can see why it's such a powerful tool for understanding network traffic.

Date: July 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 security analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who**: ME • **What**: captured network traffic using tcpdump • **Where**: in the Linux terminal • **When**: July 25, 2024 • **Why**: To monitor network traffic and analyze for malicious activity
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: July 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 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**: 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? Ensure that all endpoint devices have up-to-date antivirus and anti-malware software installed to detect and block malicious files. Also, restrict users' permissions to install or execute files, especially from unknown sources. Should we consider improving security awareness training so that employees are careful with what they click on? Absolutely. If employees are aware of potential security risks, it will be easier to avoid a data breach.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

Using tcpdump was quite challenging for me. As a newcomer to command line tools, grasping the syntax of tcpdump presented a significant learning curve. Initially, I felt quite frustrated due to the lack of correct output. However, after revisiting the activity, I was able to identify and rectify my mistakes. This experience taught me the importance of carefully reading instructions and proceeding through tasks methodically.

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

After completing this course, my comprehension of incident detection and response has significantly deepened. Initially, I possessed a rudimentary understanding of these concepts, but I was unaware of their intricate complexities. Progressing through the course, I gained insight into the lifecycle of an incident, the crucial roles of planning, processes, and people, as well as the various tools utilized in the field. Overall, I feel that my perspective has shifted, and I now possess a wealth of knowledge and insight into incident detection and response.

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

I found learning about network traffic analysis and using network protocol analyzer tools to be incredibly enjoyable. This was my first exposure to network traffic analysis, so it was a mix of both challenging and exhilarating. Being able to capture and analyze network traffic in real-time using tools was particularly fascinating. This experience has sparked a keen interest in furthering my knowledge in this area, and I aspire to enhance my proficiency in using network protocol analyzer tools in the future.