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 two phases: 1. **Detection and Analysis**: The scenario describes how the company found out about the ransomware incident. The group sought technical support from several organizations for the analytical step. 2. **Containment, Eradication, and Recovery**: Some of the actions the organization took to contain the incident are described in the scenario. For instance, the business turned off its computer systems. They nevertheless reached out to a number of other groups for help because they were unable to eliminate and recover from the catastrophe on their own.
Tool(s) used	None
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: Because of a phishing attempt, unethical hackers were able to gain access to the organization's networks and trigger the incident. The attackers started their ransomware on the company's servers after gaining access and encrypting crucial files. The ransom note the attackers left wanted a sizable sum of money in exchange for the decryption key, suggesting that their goal was financial.

Additional notes	1. How could the healthcare company prevent an incident like this from occurring again? Even if all of these tactics are crucial for defending against ransomware, you could still become a target of a successful assault. Planning makes a difference in this situation. You can recover rapidly with little damage done if the appropriate technology, software, and best practices are used. Every healthcare business needs to obtain a thorough security check-up, in my opinion, to make sure that its defenses are strong enough to fend off even the most sophisticated ransomware attacks. 2. Should the company pay the ransom to retrieve the decryption key? No. Although an attack will undoubtedly result in serious issues, I advise against ever paying a ransom. Even if you pay, cybercriminals frequently refuse to grant you access. It is worthwhile to think about purchasing ransomware insurance to lessen the harm.

Date: July 25 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	I examined a packet capture file for this action using Wireshark. Network protocol analyzer Wireshark has a graphical user interface. Because it enables security researchers to record and examine network traffic, Wireshark is valuable in the field of cybersecurity. This can aid in identifying and looking into malicious activities.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	I was eager to start this exercise and examine a packet capture file because I have used Wireshark before. The user interface was rather intimidating at first

	glance. I understand why it's a potent tool for analyzing network data.

Date: July 25 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	I used tcpdump to record and examine network traffic for this activity. A network protocol analyzer called Tcpdump can be accessible via the command-line interface. The significance of tcpdump in cybersecurity is similar to that of Wireshark in that it enables security analysts to record, filter, and examine network data.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	The command-line interface seems clear to me. It was difficult to use it to record and filter network traffic, though. I used the incorrect commands a few times, which caused me to get stuck. However, I was able to complete this exercise and record network traffic after carefully following the directions and redoing a few steps.

Date: July 27 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	The investigative tool VirusTotal, which scans files and URLs for harmful content

	like viruses, worms, trojan horses, and more, was utilized for this work. It's a great tool to use if you want to quickly determine whether other members of the cybersecurity community have flagged a website or file as malicious once it has displayed signs of compromise. I examined a file hash that had been flagged as malicious for this activity using VirusTotal. During the **Detection and Analysis** phase, an occurrence happened. I was put in the position of a security analyst at a SOC looking into a suspicious file hash in the scenario. I had to conduct more thorough research and analysis after the security measures in place identified the suspicious file to ascertain whether the alert indicated a legitimate 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? I believe the best course of action is to enhance employee security awareness training. It's crucial to periodically test your staff on what they have learned and make sure they are still adhering to cybersecurity best practices. Using an automated testing platform that simulates phishing emails and tracks whether recipients were duped by the message and engaged in dangerous conduct is an efficient approach to accomplish this. In order to reinforce their knowledge, users who fail the assessments are immediately enrolled in additional training.

Reflections/Notes:

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

The task using tcpdump was a little difficult for me. Learning the syntax for a tool like tcpdump was a terrific learning experience, and I enjoyed utilizing the command line. I initially experienced a lot of confusion because I wasn't obtaining the desired results. I redone the exercise to identify my mistakes. I took away from this experience the need to carefully follow the directions and go gently.

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

My understanding of incident detection and response has clearly changed as a result of attending this course. I had a basic understanding of detection and reaction at the start of the course, but I wasn't entirely aware of how intricate it was. As I moved through the training, I discovered the incident lifecycle, the value of strategies, processes, and people, as well as the tools employed. Overall, I believe that my understanding of incident detection and response has evolved, and I am now better informed and equipped.

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

I really enjoyed learning about network traffic analysis and using network protocol analyzer tools to put what I had learned to use. It was tough and thrilling for me to learn about network traffic analysis for the first time. The ability to employ technologies to record network traffic and analyze it in real-time greatly intrigued me. I have a greater desire to study more about this subject and eventually improve my ability to use network protocol analyzer 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.